פרק 1

תכנון ועיצוב
רשת Windows 2000

אודות פרק זה

בפרק זה תלמד כיצד לתכנן רשת מבוססת Windows 2000. בנוסף, תלמד אודות נקודות חשובות אליהן יש להתייחס בעת פיתוח אסטרטגיית הטמעה. מעבר לכך, ילמד אותך פרק זה אודות פרוטוקולי הרשת השונים הנתמכים על ידי Windows 2000, ואת יחסם לשירותי הרשת השונים.

לפני שתתחיל

להשלמת פרק זה צריך שיהיה ברשותך:

- ❖ לפרק זה אין דרישות מקדימות.

שיעור 1: סקירת שירותי הרשת

Windows 2000 מספקת מיגוון רחב של תכונות ושירותי רשת אותם יוכל הארגון שלך לנצל כדי להגיע למטרות העסקיות שלו. Windows 2000 כוללת טכנולוגיות חשובות העשויות להוסיף ערך מוסף רב לרשתות חדשות וקיימות. חלק מהטכנולוגיות חייבות להיות מיושמות ברשת שלך, כדי שניתן יהיה להשתמש במספר שירותים. לדוגמה, פרוטוקול TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) חייב להיות מותקן במערכת כדי שניתן יהיה ליישם את שירותי Active Directory של Windows 2000. פרק זה מציג את שירותי הרשת הבאים של Windows 2000:

- DNS (**D**omain **N**ame **S**ystem)
- DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol)
- WINS (**W**indows **I**nternet **N**ame **S**ervice)

בנוסף תלמד אודות רישות מרוחק, באמצעות שירותי הניתוב וגישה מרחוק (RRAS, **R**outing and **R**emote **A**ccess **S**ervice) של Windows 2000. תלמד על מתרגם כתובות הרשת (NAT, **N**etwork **A**ddress **T**ranslator) וכיצד מיושם נושא אבטחת הרשת באמצעות שירותי האישורים של Microsoft (Microsoft Certificate Services).

לאחר שיעור זה, תוכל

- להסביר את מטרת DNS, DHCP ו- WINS.
- לתאר את שירותי הניתוב וגישה מרחוק (RRAS) של Windows 2000.
- לתאר את יתרונות תרגום כתובות הרשת באמצעות NAT.
- לזהות את מאפייני שירותי האישור של Microsoft.

זמן לימוד משוער: 40 דקות

TCP/IP

Windows 2000 תומכת במיגוון רחב של פרוטוקולי רשת; אולם, פרוטוקול TCP/IP הוא הפרוטוקול העיקרי בו משתמשת Windows 2000, ומהווה את פרוטוקול ברירת המחדל לרישות, המותקן בעת התקנת מערכת ההפעלה Windows 2000. רבים משירותי הרישות של Windows 2000 משתמשים בפרוטוקול זה, ושירותים מסוימים, כגון שרת IIS (**I**nternet **I**nformation **S**erver) ו- Active Directory, דורשים את התקנתו. TCP/IP הוא פרוטוקול בר-ניתוב בו נעשה שימוש ברשתות מרחביות (WAN) רבות, ובאינטרנט. פרוטוקולים אחרים, כגון NetBEUI (**NetB**IOS **E**nhanced **U**ser **I**nterface) שאינם ניתנים לניתוב, נועדו רק לרשתות מקומיות (LAN), וכתוצאה מכך אינם תומכים בקישוריות לרשת האינטרנט. חשוב שנושא זה יילקח בחשבון בעת תכנון ועיצוב הרשת שלך.

Domain Name System

למרות ש-TCP/IP משתמש בפרוטוקול האינטרנט (IP) לאיתור ולהתחברות למארחים (Hosts, מחשבים והתקני TCP/IP אחרים ברשת), מעדיפים משתמשי המחשב לעשות שימוש בשמות ידידותיים יותר.

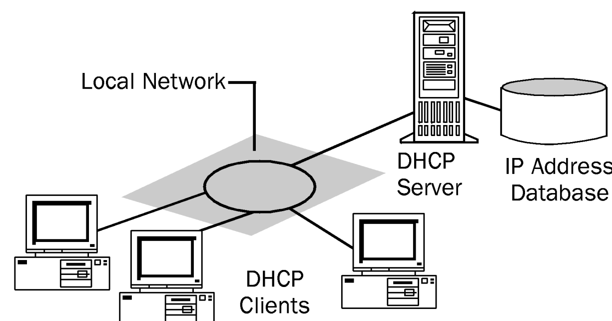
למשל, המשתמשים יעדיפו את השימוש בכתובת ftp.microsoft.com, במקום בכתובת ה-IP של השרת, 172.16.23.55.

מערכת DNS (Domain Name System) מאפשרת לך להשתמש בשמות ידידותיים, במבנה היררכי, כדי להקל עליך את האיתור והגישה למחשבים ולמשאבים אחרים ברשת מבוססת IP.

ברחבי האינטרנט מספק DNS מוסכמות תקניות למתן שמות, לאיתור מחשבים מבוססי IP. לפני יישום DNS שימש הקובץ Hosts לאיתור משאבי TCP/IP ברשתות, כולל האינטרנט. מנהלי רשתות (Network Administrators) הוסיפו שמות וכתובות IP לקובץ Hosts והמחשבים ברשת נעזרו בקובץ זה לצורך הסדרת השמות (Name Resolution).

Dynamic Host Configuration Protocol

DHCP מפשט את נושא ניהול ותחזוקת כתובות IP ברשת מבוססת TCP/IP, על ידי אוטומציית הגדרות הכתובת עבור הלקוחות. כשרת DHCP יכול להיחשב כל מחשב בו פועל שירות DHCP. שרת Windows 2000 מספק את שירות שרת DHCP, המאפשר למחשב לתפקד כשרת DHCP ולהגדיר לקוח המאפשר DHCP (DHCP-Enabled Client) ברשת שלך.



תרשים 1.1 מודל DHCP בסיסי

שירות שרת DHCP בסביבת Windows 2000 מספק גם :

- ❖ שילוב עם שירותי Active Directory ו-DNS
- ❖ ניטור מתקדם ודיווח סטטיסטי
- ❖ אפשרויות ייחודיות ליצרן ותמיכה במחלקות-משתמש
- ❖ הקצאת כתובות Multicast
- ❖ זיהוי שרת DHCP מתחזה

לכל מחשב ברשת מבוססת TCP/IP חייבת להיות כתובת IP ייחודית, כדי שיוכל לגשת לרשת ולמשאבים המשותפים בה. כאשר לא נעשה שימוש בשרת DHCP יש לבצע את כל הגדרות IP באופן ידני בכל מחשב חדש, במחשבים העוברים מ-Subnet אחת לאחרת, ומחשבים המוסרים מהרשת. על ידי יישום DHCP ברשת, תהליך ההגדרה יהיה כולו מבוצע באופן אוטומטי ומנוהל מנקודה מרכזית אחת.

יישום DHCP קשור בקשר הדוק ל-WINS ול-DNS, כך שמנהלי רשתות רק ירוויחו משילוב כל השלושה יחד בעת תכנון ההטמעה. אם אתה משתמש בשרתי DHCP עבור לקוחות רשת של Microsoft, עליך להשתמש בשירות להסדרת שמות (Name Resolution Service). רשתות מבוססות Windows 2000 משתמשות בשירות DNS כדי לתמוך ב- Active Directory, בנוסף להסדרת שמות כללית. רשתות התומכות בלקוחות Windows NT 4.0 או קודמות לה, צריכות להשתמש בשרתי WINS. רשתות המשלבות לקוחות Windows 2000 ולקוחות Windows NT 4.0 צריכות ליישם הן WINS והן DNS.

Windows Internet Name Service

WINS הוא שרת שמות המשמש מערכות הפעלה כגון Windows NT 4.0, או קודמות לה. WINS מספק מסד נתונים מבוזר לרישום ולאיתור שם מחשב (שהוא זהה לשם NetBIOS) למיפוי כתובת IP בסביבת רשת מנותבת. אם אתה מנהל רשת מבוזרת, WINS יהיה בחירתך הטובה ביותר לשם הסדרת שמות NetBIOS. WINS מפחית את השימוש ב- Local Broadcast לצורך הסדרת שמות, ומאפשר למשתמשים לאתר בקלות מערכות ברשתות מרוחקות. בסביבת DHCP דינמית, יכולות כתובות IP של המארחים להשתנות לעיתים קרובות; WINS מספק דרך לרישום דינמי של השינויים במיפויי שמות מחשבים לכתובות ה-IP שלהם. תכונה זו נדרשת כדי שהסדרת שמות NetBIOS לכתובות IP תפעל כהלכה בסביבת DHCP.

Name Resolution

בין אם הרשת שלך משתמשת ב-WINS או ב-DNS, נושא הסדרת השמות מהווה חלק חשוב מאוד בעבודת הניהול שלך. למרות שבעיקרה משתמשת Windows 2000 ב-DNS לשם התאמת שמות המארחים לכתובות ה-IP, היא עדיין תומכת גם ב-WINS לצורך זה.

הסדרת שמות (Name Resolution) מאפשרת לך לחפש ברשת שלך ולהתחבר למשאבים שלהם שמות כגון: printer1 או fileserver1, במקום שתידרש לזכור בעל פה את כתובת ה-IP של המשאב. יעיל אף פחות יהיה לנסות ולזכור את כתובת ה-IP, כאשר משתמשים ב-DHCP להקצאת כתובות, מפני שהקצאה עשויה להשתנות במשך הזמן. WINS משולב בהדיקות עם שירותי DHCP. בשל שילוב הדוק זה, בכל פעם שהמחשב fileserver1 מקבל באופן דינמי הקצאה של כתובת IP חדשה, השינוי שקוף לגמרי. כאשר אתה מתחבר למחשב fileserver1 מרכיב רשת (Node) אחר, אתה יכול להשתמש בשם fileserver1 במקום בכתובת ה-IP החדשה, מפני ש-WINS עוקב אחר השינויים בכתובות ה-IP המשוייכות לשם זה.

סקירת הגישה מרחוק

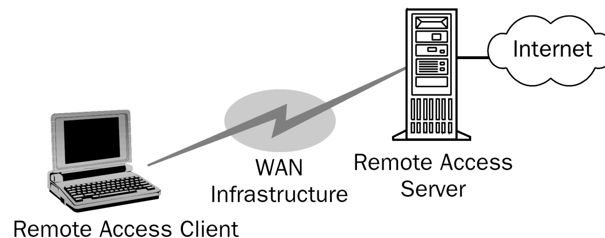
באמצעות התכונה ניתוב וגישה מרחוק (Routing and Remote Access) של Windows 2000, לקוחות מרוחקים מתחברים באופן שקוף לשרת המרוחק, דבר הידוע גם בשם **גישה מרחוק מנקודה-לנקודה** (Point-to-Point Remote Access Connectivity). מחשבי לקוח יכולים גם להתחבר באופן שקוף לרשת אליה מחובר שרת הניתוב וגישה מרחוק (Routing and Remote Access Server). דבר זה ידוע גם בשם **גישה מרחוק מנקודה-לרשת מקומית**

(Point-to-LAN Remote Access Connectivity). חיבור שקוף זה מאפשר למחשבי לקוח לחייג ממיקומים מרוחקים ולבצע גישה למשאבים, ממש כאילו היו מחוברים באופן פיסי לרשת. גישה מרחוק של Windows 2000 מאפשרת שני סוגי גישה מרחוק:

- **גישה מרחוק בחיוג** (Dial-up Remote Access). בגישה מסוג זה נעזר המשתמש בתשתית הטלפוניה ליצירת חיבור פיסי או וירטואלי זמני ליציאה (Port) בשרת הגישה מרחוק. לאחר שנוצר החיבור הפיסי או הווירטואלי, ניתן לשאת ולתת לגבי יתר פרמטרי ההתחברות.
- **גישה מרחוק ב-VPN** (Virtual Private Network Remote Access). בגישה מסוג זה נעזר לקוח VPN ברשת ציבורית מבוססת IP כדי ליצור חיבור וירטואלי מנקודה-לנקודה עם שרת גישה מרחוק, הפועל גם כשרת VPN. לאחר שנוצר החיבור הווירטואלי מנקודה-לנקודה, ניתן לשאת ולתת לגבי יתר פרמטרי ההתחברות.

מרכיבים בחיבור גישה מרחוק בחיוג

שירות הניתוב וגישה מרחוק (RRAS, **R**outing and **R**emote **A**ccess **S**ervice) של Windows 2000 מקבל חיבורים בחיוג ומעביר מנות (Packets) בין לקוחות גישה מרחוק והרשת אליה מחובר שרת הגישה מרחוק. חיבור מרחוק כולל לקוח גישה מרחוק, תשתית רשת מרחבית (WAN) ושרת גישה מרחוק, כפי שמתואר בתרשים 1.2.



תרשים 1.2 מרכיבים בחיבור גישה מרחוק בחיוג

פרוטוקולים לגישה מרחוק

פרוטוקולים לגישה מרחוק שולטים ביצירת הקישור ובהעברת הנתונים דרך קישורי WAN. מערכת ההפעלה ופרוטוקולי LAN המותקנים בלקוחות ובשרתי הגישה מרחוק מכתיבים באיזה פרוטוקול גישה מרחוק ישתמשו הלקוחות שלך.

שירות הניתוב וגישה מרחוק של Windows 2000 תומך בשלושה סוגי פרוטוקולי גישה מרחוק:

1. PPP (**P**oint-to-**P**oint **P**rotocol) הוא קבוצת פרוטוקולים המאוגדים בתקן תעשייתי ומספקים את רמת האבטחה הטובה ביותר, תמיכה בריבוי פרוטוקולים, יכולת פעולה הדדית בין מחשבים שונים ותמיכה בקבלת כתובת IP בצורה דינמית.
2. SLIP (**S**erial **L**ine **I**nternet **P**rotocol) משמש בעיקר שרתי גישה מרחוק מיושנים. SLIP אינו תומך בקבלת כתובת IP בצורה דינמית.

3. פרוטוקול שירות הגישה מרחוק של Microsoft (הידוע גם בשמו Asynchronous NetBEUI או בקיצור AsyBEUI) הוא פרוטוקול גישה מרחוק בו משתמשים לקוחות גישה מרחוק מיושנים, הפועלים בסביבת מערכות הפעלה כגון Windows NT 3.1, Windows for Workgroups, MS-DOS או LAN Manager.

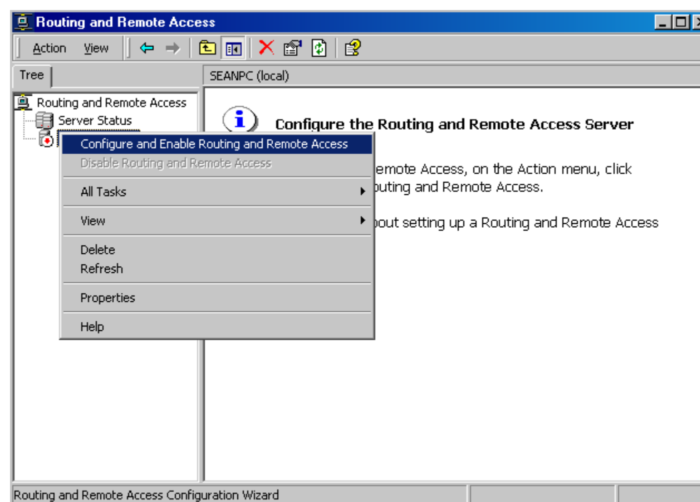
פרוטוקולי LAN הם אלה המשמשים את לקוחות הגישה מרחוק לגשת למשאבים ברשת המחוברת לשרת הגישה מרחוק. גישה מרחוק של Windows 2000 תומכת בפרוטוקולים TCP/IP, IPX, AppleTalk ו-NetBEUI.

➢ כדי להגדיר שרת ניתוב וגישה מרחוק:

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ולחץ על Routing and Remote Access.

2. לחץ לחיצה ימנית על השרת שבחלונית השמאלית, ומתפריט הקיצור בחר Configure and Enable Routing and Remote Access, כפי שמוצג בתרשים 1.3.

על המסך מופיע חלון Routing and Remote Access Server Setup Wizard, המאפשר לך לציין נתוני הגדרת שרת.



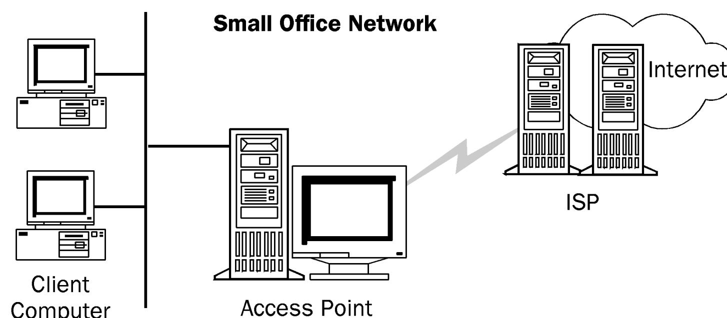
תרשים 1.3 יצירת שרת ניתוב וגישה מרחוק

Network Address Translator

קיימים שני סוגי כתובות IP: ציבוריות ופרטיות. כתובות ציבוריות מוקצות עבורך על ידי ספק שירותי האינטרנט (ISP, **I**nternet **S**ervice **P**rovider) המספק לך את החיבור לאינטרנט. עבור מארחים בארגון שאינם דורשים גישה ישירה לאינטרנט, יש להקצות כתובות IP שאינן מקבילות לכתובות IP ציבוריות הקיימות כבר באינטרנט. כדי לפתור בעיית מיעון זו, שימרו מעצבי האינטרנט חלק ממרחב כתובות ה-IP וקראו לו בשם מרחב כתובות פרטי (Private Address Space). כתובת IP פרטית לעולם אינה מוקצית כמו כתובת

IP ציבורית. כתובות IP מתוך מרחב הכתובות הפרטי ידועות ככתובות פרטיות (Private Addresses). תוך שימוש בכתובות IP פרטיות ניתן להגן על הרשת מפני פריצות.

מכיון שכתובות ה-IP ממרחב הכתובות הפרטיות לעולם לא יוקצה על ידי InterNIC (**Inter**net **N**etwork **I**nformation **C**enter) ככתובות ציבוריות, לעולם לא יהיו קיימים בנתבי האינטרנט (Internet Routers) נתיבים (Routs) עבור כתובות פרטיות. כתובות פרטיות אינן נגישות מתוך האינטרנט. בשל כך, כאשר משתמשים בכתובות IP פרטיות, עליך להיעזר בסוג כלשהו של שרת Proxy, כדי להמיר את טווח(י) הכתובות הפרטיות ברשת הפנימית שלך לכתובות IP ציבוריות אותן ניתן לנתב. אפשרות אחרת היא לתרגם את הכתובות הפרטיות לכתובות ציבוריות חוקיות באמצעות מתרגם כתובות רשת (NAT, **N**etwork **A**ddress **T**ranslator), לפני שהן נשלחות באינטרנט. התמיכה בתרגום כתובות רשת לשם תרגום כתובות פרטיות וציבוריות, כדי לאפשר קישור של משרד קטן או משרד ביתי לאינטרנט, מתואר בתרשים 1.4.



תרשים 1.4 קישור רשת משרדית קטנה לאינטרנט

NAT מסתיר כתובות IP המנוהלות באופן פנימי מרשתות חיצוניות, על ידי תרגום הכתובת הפרטית הפנימית לכתובת ציבורית חיצונית. דבר זה מפחית את עלויות רישום כתובות IP על ידי כך שהלקוחות יכולים להשתמש בכתובות פנימיות פרטיות בחלק הפנימי של הרשת, ותרגומן של מספר קטן של כתובות לכתובות IP רשומות (ציבוריות) כלפי חוץ. בנוסף, תרגום שכזה מסתיר את מבנה הרשת הפנימי, וכך מפחית את הסיכון של חדירה למערכות בתוך הארגון.

שירותי אישורים

עיצוב מערכת אבטחה מתאימה להגנה על המידע החשוב והפרטי של הארגון שלך דורש פיתוח ערכת פתרונות המתאימים לתרחישי סיכון מסוימים. Windows 2000 מספקת מיגוון טכנולוגיות מהן תוכל לבחור בעת תכנון אסטרטגיית האבטחה שלך. אחת מטכנולוגיות אלו היא שירותי האישורים של Microsoft (Microsoft Certificate Services). תוכל ליישם את שירותי האישור כדי ליצור ולנהל רשות אישורים (CA, **C**ertificate **A**uthority) המנפיקה אישורים דיגיטליים.

אישורים דיגיטליים (Digital Certificates) הם אישורים אלקטרוניים (Electronic Credentials) המבטיחים את זהותם המקוונת של יחידים, ארגונים ומחשבים. אישורים אלה מתפקדים בדומה לתעודות זהות, דרכונים או רישיונות נהיגה. כאשר מוצגת תעודת זהות לגורמים אחרים הם יכולים לוודא את זהות בעליה, מפני שהתעודה מספקת את יתרונות האבטחה הבאים:

- ❖ היא מכילה מידע המאפשר לזהות ולאתר את בעליה.
- ❖ היא מכילה את החתימה של הבעלים המורשים, כדי לאפשר זיהוי ודאי.
- ❖ היא מכילה את המידע הנדרש לשם זיהוי והתקשרות עם הרשות המאשרת.
- ❖ היא מעוצבת כך שקשה מאוד יהיה לזייף אותה.
- ❖ היא מונפקת על ידי רשות אשר יכולה לבטל את תוקפה בכל עת (למשל, אם נעשה בה שימוש שלא על פי חוק, או שהיא נגנבה).
- ❖ ניתן לבדוק את תוקפה על ידי התקשרות עם מנפיק התעודה.

אישורים דיגיטליים יכולים לשמש בדרך דומה גם כדי לספק מיגוון תפקודי אבטחה. תפקודי האבטחה השכיחים בהם ניתן להשתמש כוללים, בין השאר:

- ❖ דואר אלקטרוני מאובטח.
- ❖ תקשורת מאובטחת בין לקוחות ושרתי אינטרנט.
- ❖ חתימה על קוד תוכנה, לשם הפצת תוכנה ברשת ציבורית.
- ❖ אימות כניסה לרשת מקומית או לגישה מרחוק.
- ❖ אימות IPSec.

שירותי אישורים (Certificate Services) מספקים לארגון את האמצעים להקים בקלות רשות אישורים (CA) כדי לתמוך בדרישות העסקיות שלהם. שירותי אישורים כוללים מודול מדיניות ברירת מחדל להנפקת אישורים ליישויות ארגוניות, כגון משתמשים, מחשבים או שירותים.

סיכום שיעור

Windows 2000 כוללת מספר טכנולוגיות עיקריות המוסיפות ערך מוסף לרשתות מבוססות TCP/IP קיימות וחדשות. למרות ש-TCP/IP משתמש ב-IP לאיתור ולהתחברות למארחים (Hosts), מעדיפים המשתמשים להשתמש בשמות ידידותיים. DNS מאפשר לך להשתמש בשמות היררכיים וידידותיים המקלים על איתור מחשבים ומשאבים ברשת מבוססת IP. DHCP מפשט את נושא ניהול הכתובות ברשת TCP/IP, על ידי הגדרה אוטומטית של כתובות עבור לקוחות הרשת. WINS מספק מסד נתונים מבוזר לרישום ואיתור שם מחשב (שהוא זהה לשם NetBIOS של המחשב) למיפוי כתובת IP בסביבת רשת בת-ניתוב. באמצעות שירות גישה מרחוק של Windows 2000, לקוחות יכולים להתחבר באופן שקוף למשתמש אל שרת גישה מרחוק (Remote Access Server). יכולים מחשבי הלקוח גם להתחבר בצורה שקופה לרשת אליה מחובר שרת הניתוב והגישה מרחוק.

שיעור 2: פיתוח תוכנית להטמעת רשת

יישום טכנולוגיות חדשות בסביבת רשת ארגונית דורש מחקר, תכנון, אישור ותקציבים. כדי להשיג את מירב היתרונות של Windows 2000 עליך לתכנן את ההטמעה ביסודיות. כאשר אתה מתחיל את תכנון הטמעת מערכת ההפעלה Windows 2000 עליך להבין את תכונותיה, כך שתוכל לנצל אותן לטובתך. דבר זה יסייע לעובדים בארגון להגדיל את פוריותם בעבודה, ויפחית את עלות הבעלות הכוללת (**T**otal **C**ost of **O**wnership ,TCO). בשיעור זה תלמד כיצד יש לתכנן את הטמעת רשת Windows 2000.

לאחר שיעור זה, תוכל

- לתאר את המהדורות השונות של מערכת ההפעלה Windows 2000.
- לתאר את השלבים במעגל החיים של פרויקט הטמעת הרשת.
- לזהות שיקולי חומרה ותוכנה בעת עיצוב הרשת.
- לזהות נושאים הקשורים בשילוב פרוטוקולי רשת מיושנים ומערכות מיושנות.

זמן לימוד משוער: 40 דקות

שיקולי מערכת ההפעלה

כאשר אתה מתכנן את רשת Windows 2000 שלך, עליך לקחת בחשבון את סוגי מערכות הפעלה, בהתאם לצרכי המשתמשים שלך ודרישות הארגון. לדוגמה, אם השרתים שלך מפעילים יישומים הדורשים כמות גדולה של זיכרון ומעמיסים על עבודת המעבד, יהיה Windows 2000 Advanced Server הבחירה הנבונה ביותר. עליך לסקור תכונות טכנולוגיות ייחודיות ל- Windows 2000 כדי לקבוע אילו טכנולוגיות הן החשובות ביותר לארגון שלך, ובה בעת לשקול את יעדי הארגון לטווח הקרוב והרחוק. הסעיפים הבאים מתארים את המהדורות השונות של מערכת ההפעלה Windows 2000.

Windows 2000 Professional

Windows 2000 Professional היא מערכת הפעלה שולחנית המשלבת את התכונות המתקדמות של Windows NT, בנוסף לאבטחה ועמידות בפני תקלות (Fault Tolerance), עם קלות השימוש ב- Windows 98, כולל תמיכה בהתקני הכנס-הפעל (Plug and Play). ניתן לשדרג ל- Windows 2000 Professional מערכת הפועלת בסביבת Windows NT Workstation גירסה 3.51 ומעלה, או Windows 98.

דרישות המערכת המינימליות של Windows 2000 Professional כוללות:

- **מעבד Pentium במהירות 133MHz או יותר.** Windows 2000 Professional תומכת במערכת בה עד שני מעבדים.
- **64MB זיכרון RAM**. ככל שכמות הזיכרון גדלה, כך משתפרים ביצועי המערכת.
- **כונן דיסק קשיח בנפח 2GB.** צריך להיות בכונן נפח פנוי של לפחות 650MB להתקנת Windows 2000 Professional.

Windows 2000 Server

Windows 2000 Server בנוי על התכונות החזקות של מערכת ההפעלה Windows NT Server גירסה 4.0. Windows 2000 Server משלב בין שירותי Directory, אינטרנט, יישומים, תקשורת, קבצים ומדפסות, באמינות גבוהה, ניהול יעיל ותמיכה בחומרת הרישות המתקדמת ביותר, כדי לספק את היסוד הטוב ביותר לשילוב רשת תקשורת המחשבים של העסק שלך עם האינטרנט. תכונות אלו כוללות, בין השאר:

- ❖ שירותי מידע אינטרנט גירסה 5.0 (IIS)
- ❖ סביבת תכנות לדפי ASP (**A**ctive **S**erver **P**ages)
- ❖ מנתח XML
- ❖ Windows DNA 2000
- ❖ COM+ (**C**omponent **O**bject **M**odel +)
- ❖ פלטפורמת מולטימדיה
- ❖ Directory-Enabled Applications
- ❖ תיקיות אינטרנט (Web Folders)
- ❖ קבלת ושליחת הדפסות דרך האינטרנט

דרישות המערכת המינימליות של Windows 2000 Server כוללות:

- ❖ **מעבד Pentium במהירות 133MHz או יותר.** Windows 2000 Server תומך במערכת בה עד ארבעה מעבדים.
- ❖ **128MB זיכרון RAM.** מומלץ שיותקנו במערכת 256MB זיכרון RAM. ככל שכמות הזיכרון גדלה, כך משתפרים ביצועי המערכת. Windows 2000 Server תומך ב-עד 4GB זיכרון RAM.
- ❖ **כונן דיסק קשיח בנפח 2GB.** צריך להיות בכונן נפח פנוי של לפחות 1GB להתקנת Windows 2000 Server. אם מתבצעת התקנה מהרשת יש צורך בשטח פנוי נוסף.

Windows 2000 Advanced Server

Windows 2000 Advanced Server הוא הגירסה החדשה של Windows NT Server 4.0 במהדורת Enterprise שלו. Windows 2000 Advanced Server הוא השרת האידיאלי ליישומים עסקיים כבדים וליישומי מסחר אלקטרוני (E-Commerce), בהם הדרישות לאפשרויות צמיחה ולזמינות גבוהה הן מחמירות ביותר. בעוד שדרישות החומרה עבור Windows 2000 Advanced Server זהות לאלו של Windows 2000 Server, שרת זה כולל גם:

- ❖ כל תכונות Windows 2000 Server
- ❖ איזון עומסים ברשת TCP/IP (Network (TCP/IP) Load Balancing)
- ❖ תמיכה ב-עד 8GB זיכרון ראשי במערכות מבוססות Intel **P**age **A**ddress **E**xtention (PAE)
- ❖ תמיכה ב-עד שמונה מעבדים

הערה ודא כי אתה מתיר מספיק זמן להתקנת Windows 2000 Advanced Server, **מכיון** שהתהליך עשוי לארוך מספר שעות.

Windows 2000 Datacenter Server

מערכת הפעלה נוספת המושתתת על תכונותיו של Windows 2000 Advanced Server היא Windows 2000 Datacenter Server. מערכת הפעלה זו תומכת ב- עד-32 מעבדים וביותר זיכרון RAM מאשר יתר מהדורות מערכת ההפעלה. תמיכה זו כוללת:

- 32GB זיכרון RAM במערכות מבוססות מעבדי Alpha
- 64GB זיכרון RAM במערכות מבוססות מעבדי Intel

במידה ועליך לתמוך בכמות גבוהה של עיבוד עסקאות מקוונות (OLTP, **O**n**l**ine **T**ransaction **P**rocessing), במחסני נתונים גדולים במיוחד ובספק שירותי אינטרנט או ספק שירותי יישומים (ISP ו- ASP), שקול את התקנת Windows 2000 Datacenter Server.

שלבים בהטמעה

מטרתו של תהליך תכנון רשת Windows 2000 שלך היא להבטיח שרשת זו תתפקד בהתאם לצרכים שלשמה נוצרה. כאשר אתה מתכנן ומעצב את הטמעת רשת Windows 2000 שלך, עליך לעבור תהליך או מעגל חיים (Life Cycle). השלבים של פרויקט מעגל חיים זה צריכים לכלול את הדברים הבאים:

1. **אבחון.** בעת שלב האבחון (Analysis) עליך לקבוע מטרות ויעדים בתחום טכנולוגיות המידע (IT). דבר זה יסייע בידך לעצב את הרשת כך שתתמוך ברוחב הפס הזמין לה, תתאים לדרישות אבטחת המידע, תאמוד את העלות מול היתרונות ולבסוף תביא לתוצאה המתאימה לארגון שלך.
2. **עיצוב.** במהלך שלב העיצוב (Design) הערך את עיצוב תשתית Windows 2000. הדבר כולל תכונות כגון DNS, WINS, DHCP ופרוטוקולי רשת. העיצוב שלך יהיה מבוסס על האבחון שביצעת, נושאי יכולת פעולה הדדית בין מחשבים שונים ותכונות נדרשות.
3. **בדיקה.** בעת שלב הבדיקה (Testing) הפעל פרויקט ניסיוני ברשת Windows 2000 שעיצבת בסביבת עבודה רגילה, עם מספר מצומצם של משתמשים. ייתכן שיהיה עליך להתאים את העיצוב שלך, בהתאם לתוצאות אותו פרויקט ניסיוני, כדי להשיג סביבת רשת המתפקדת ביציבות הרצויה.
4. **יישום.** שלב היישום (Production) הוא השלב האחרון בתהליך ההטמעה של Windows 2000. הרשת נבדקה בתוכנית ניסיונית בהתאם לעיצוב שלך, וכעת אתה מוכן להטמיע את Windows 2000 בכל רחבי הארגון. במהלך שלב זה, צור תוכנית להתאוששות מאסון וספק חומר לימוד למשתמשים ולאנשי מרכז התמיכה בארגון.

חומרה

נושאי תאימות חומרה ותוכנה עלולים לגרום לפשרה בתחומי אמינות ואיכות. תוכל לבחון את תאימות החומרה והתוכנה שלך עם Windows 2000 באתר האינטרנט שכתובתו: http://www.microsoft.com/windows2000/default.asp.

לפני שתטמיע את Windows 2000, עליך לבצע רישום מדויק של מלאי החומרה והתוכנה המותקנים בכל השרתים ובמחשבי הלקוח בארגון. ברישומים אלה עליך לכלול גם הגדרות מדויקות של ה-BIOS (**B**asic **I**nput/**O**utput **S**ystem). בנוסף, עליך לכלול גם רישום מדויק של הגדרות ותצורת הציוד ההיקפי, גרסאות מנהלי התקנים (Drivers), חבילות שירות (Service Pack, במידה ומותקנות) ונתוני תוכנה וקושחה (Firmware) נוספים. מעבר לכך, נסה ליצור תקן תצורה (Configuration Standard) למחשבי השרתים והלקוחות בארגון. תקן זה אמור לקבוע קווים מנחים לרכישת ציוד, דרישות סף למהירות מעבדים, דרישות סף לכמות זיכרון RAM בכל מחשב, נפח סף של כונני דיסק קשיח מקומיים וציוד היקפי, כגון כונני תקליטורים או מערכות אל-פסק.

ודא שכל התקני הרישות בארגון, כגון רכזות (Hubs) וחיווט (Cabling), מהירים דיים לצרכיך. אם הארגון שלך מעביר קול ווידאו באמצעות חיווט הרשת שלך, אז החיווט והמתגים (Switches) שבדרך חייבים לתמוך ברוחב הפס הנדרש עבור שירותים אלה. משתמשים מרוחקים מסוימים אינם יוצרים תעבורת רשת גבוהה במיוחד. למשל, משתמש מרוחק העובד על מסמך Word או על גיליון Excel אינו יוצר תעבורת רשת גבוהה לשרת הניתוב וגישה מרחוק, כמו שהיה יוצר אם היה ניגש למסדי נתונים ולמערכות פיננסיות. בשל כך ייתכן כי כבל מסוג Category-3 במהירות 10-Mbps ועם רכזת מתאימה עשוי להתאים למצבים מסוימים, בעוד שבמצבים אחרים, כגון במקרה של שימוש ביישומים הדורשים תעבורת רשת גבוהה, ייתכן שיידרשו כבלים מסוג Category-5 במהירות 100-Mbps, והתקני רשת מתאימים. נסה לרשום לפניך את רוחב הפס הזמין בשעות העומס, בשעות העבודה הרגילות (העמוסות מעט פחות) ובשעות בהן אין עומס (בדרך כלל בלילה).

תאימות עם מערכות מיושנות

רשתות רבות הן הטרוגניות, כלומר הן תערובת של מערכות הפעלה ופרוטוקולי רשת. למשל, מחשבי Windows 2000 שלך עשויים לתקשר עם מארחי Mainframe, מערכות UNIX או מערכות הפעלה לרשת אחרות. בעת התכנון, עליך לרכז את נושאי יכולת הפעולה ההדדית בין מחשבים שונים, אל מול המערכות החשובות ביותר בארגון.

בנוסף, Windows 2000 Server מציע שירותי Gateway למערכות הפעלה אחרות, מה שמאפשר לך לגשת למשאבי רשת. Gateway Service for NetWare, למשל, מאפשר ללקוחות רשת Windows 2000 שלך לנווט בין היררכיות NDS (**N**ovell **D**irectory **S**ervices), להשתמש בתסריטי כניסה של נובל גירסה 4.2 ומעלה ואפילו לקבל אימות משרת נובל.

שיקולים בבחירת פרוטוקולי רשת

רשתות מסוימות עושות שימוש במיגוון פרוטוקולים, בהתאם לצרכים. לדוגמה, רשת Ethernet קטנה עשויה להשתמש בפרוטוקול NetBEUI כפרוטוקול LAN, בעוד שהיא תעשה שימוש בפרוטוקול TCP/IP לצורך הקישוריות לאינטרנט. בנוסף על כך, רשתות הכוללות

שרתי NetWare של נובל וגם שרתי Windows NT תשתמשנה בפרוטוקולים IPX/SPX (NWLink) ו-TCP/IP. בחן תמיד את הפרוטוקולים בהם נעשה שימוש ברשת שלך, ושקול אם ניתן להחליף כל אחד מהם, או אפילו לבטל, בעת המעבר ל- Windows 2000. למשל, אם אתה משדרג לקוחות המשתמשים ב- IPX/SPX ל- Windows 2000 Professional (NWLink), ייתכן שניתן לבטל את השימוש בפרוטוקול IPX/SPX (NWLink) ברשת שלך.

Windows 2000 מכילה חבילת פרוטוקולים TCP/IP בעלת תפקודיות רבה יותר מאשר גרסאות קודמות של Windows. כדי שתוכל להשתמש בשירותי Active Directory ולנצל את התכונות המתקדמות של Windows 2000 חובה עליך להתקין את פרוטוקול TCP/IP. בשל כך, עליך לשקול את הפשטת הרשת שלך על ידי שימוש בפרוטוקול TCP/IP בלבד.

את נתוני הרשת והגדרותיה בסביבת Windows NT תוכל לאתר על ידי לחיצה ימנית על סמל My Computer בשולחן העבודה, ומתפריט הקיצור לבחור Properties.

סיכום שיעור

עליך לתכנן את צעדי ההטמעה בקפידה, כדי להשיג את כל יתרונות מערכת ההפעלה Windows 2000, ולהכיר את ההבדלים שבין מהדורות מערכת ההפעלה. הטמעת רשת ארגונית כוללת מספר שלבים בפרויקט מעגל החיים: אבחון, עיצוב, בדיקה ויישום. לפני יישום Windows 2000, ערוך רשימת מלאי של כל החומרה והתוכנה המותקנים בכל אחד ממחשבי השרת ומחשבי הלקוח המחוברים לרשת שלך. בנוסף, שקול נושאי פעולה הדדית של מערכות שונות וקבע אילו פרוטוקולים יענו לצרכיך.

שיעור 3: פרוטוקולים שכיחים הנתמכים על ידי Windows 2000

כאשר אתה מתכנן רשת, עליך לשקול את דרישות ההתחברות של המשתמשים שלך. פרוטוקולי רשת הם כמו שפה, במובן שלשפות שונות יש מילים שונות, מבנה מילה שונה וניקוד שונה. פרוטוקול רשת משמש בתפקיד דומה עבור מחשבים המנסים לתקשר ביניהם. פרוטוקול הרשת בו נעשה שימוש קובע כיצד יוגדרו ויישלחו המנות (Packets, יחידות נתונים) דרך כבלי הרשת. שקול את השאלות הבאות:

- **האם לקוחות ברשת מתחברים לשרתי NetWare של נובל?** לקוחות המתחברים לשרתי NetWare חייבים להשתמש בפרוטוקול NWLink. אפילו אם שרתי NetWare מוגדרים לעבודה עם פרוטוקול TCP/IP, לקוחות מבוססי Windows חייבים להשתמש בפרוטוקול NWLink כדי לתקשר עימם.
- **האם הרשת שלך מחוברת באמצעות נתבים?** פרוטוקול NetBEUI הוא פרוטוקול שאינו בר-ניתוב. כדי שמחשבים משני צידי נתב (Router) יוכלו לתקשר ביניהם עליהם להשתמש בפרוטוקול בר-ניתוב (Routable Protocol), כגון: TCP/IP או NWLink.
- **האם אתה מחובר לאינטרנט?** כדי שלקוחות יוכלו להתחבר לאינטרנט, חייב להיות מותקן בהם פרוטוקול TCP/IP.

מעבר לכל זה, תכונות מסוימות דורשות את התקנתם של פרוטוקולים מסוימים. אם אתה מעוניין להשתמש בשירותי Active Directory, להשתמש ב-IIS או לספק ללקוחות הרשת שלך גישה לאינטרנט, עליך להתקין את פרוטוקול TCP/IP. שיעור זה יתאר את פרוטוקול TCP/IP ופרוטוקולים אחרים בהם ניתן להשתמש בסביבת Windows 2000.

לאחר שיעור זה, תוכל

- לזהות ארכיטקטורות רשת שונות.
- לזהות את הפרוטוקולים השונים בהם עושה Windows 2000 **שימוש.**

זמן לימוד משוער: 30 דקות

TCP/IP

Transmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol (TCP/IP) היא בעצם חבילת פרוטוקולים המוגדרים כתקן תעשייתי (Industry Standard) שנועדה לשימוש ברשתות גדולות. TCP/IP הוא פרוטוקול בר-ניתוב, מה שאומר שניתן למתג (Switch) מנות נתונים (לנתב אותן בין Subnets שונות) תוך שימוש בכתובת היעד של המנה. יכולתו של TCP/IP להיות מנותב מספקת Fault Tolerance, שהיא יכולתו של מחשב או של מערכת הפעלה להגיב לאירוע חריג או לתקלה, כגון הפסקת חשמל או כשל בחומרה, ובכך להבטיח שהנתונים אינם אובדים או מושחתים. אם מתרחשת תקלת רשת, מנותבות מנות הנתונים של TCP/IP לנתיב חלופי.

למרות שהמטרה המקורית ביצירת פרוטוקול TCP/IP היתה לספק קישוריות בין רשתות שונות לגמרי, כיום מספק TCP/IP קישור מהיר בין רשתות. Microsoft יישמה את TCP/IP כפרוטוקול התקני לרשתות מבוססות Windows 2000. בפרק 2 תלמד בהרחבה אודות ארכיטקטורת הפרוטוקול, התקנתו והגדרתו.

יתרונות ביישום TCP/IP

TCP/IP בסביבת Windows 2000 כולל שיפורים רבים בתחום רשתות רחבות פס. תכונות אלו מפורטות בסעיפים הבאים.

תמיכה בחלון גדול

גודל החלון בתקשורת מבוססת TCP הוא מספר המנות המירבי שניתן לשלוח לפני שצריך לשלוח אישור קבלה (Acknowledge) למנה הראשונה. גודל החלון (Window Size) הוא בדרך כלל קבוע, ונקבע בתחילת השיח (Session) בין המערכת השולחת והמערכת המקבלת. בתמיכה בחלון גדול, גודל החלון מחושב באופן דינמי מחדש, ומוגדל, אם לאורכו של שיח ממושך נשלחות מספר רב של מנות. דבר זה מגדיל את רוחב הפס (Bandwidth) ומאפשר למספר גדול יותר של מנות נתונים להיות מועברות ברשת בכל רגע נתון.

אישור קבלה ברריני

במקרה של אישורי קבלה ברריניים (Selective Acknowledgments), יכול המקבל להודיע ולבקש מנות מסוימות שלא הגיעו ליעדן ו/או הגיעו מהשולח כשהן אינן תקינות. דבר זה מאפשר לרשתות להתאושש במהירות ממצב של יתירות זמנית (Temporary Congestion), או הפרעות, מפני שאז נשלחות פעם נוספת רק המנות הנדרשות. ביישומים קודמים של TCP/IP, אם הצד המקבל לא קיבל ולו מנת TCP אחת, היה השולח צריך לשדר פעם נוספת את כל מנות הנתונים שאחרי המנה המופיעה באישור הקבלה, המכיל את המנה השגויה. תוך שימוש באישור קבלה ברריני נשלחות פחות מנות נתונים שליחה חוזרת, ובכך מטיבות עם ביצועי הרשת וניצולה.

הערכת משך הלוך-חזור

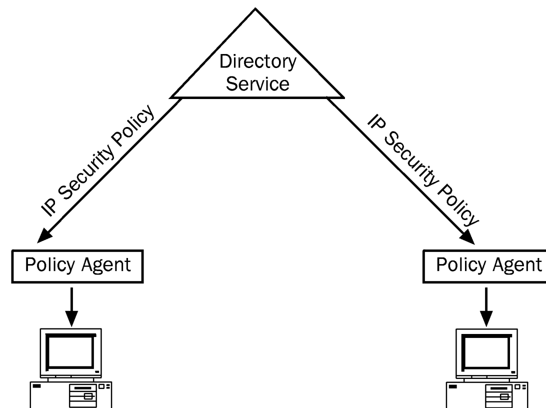
משך הלוך-חזור (Round Trip Time ,RTT) הוא משך הזמן שייקח למנה לבצע את המהלך בין שני הצמתים המתקשרים (Sender ו- Receiver), הלוך וחזור בקישור מבוסס TCP. הערכת RTT היא טכניקה להערכת משך הזמן שייקח למנת נתונים לבצע את ה"טיול" והתאמת משך הזמן האופטימלי של המסע. מאחר והביצועים מושפעים מהידיעה של כמה זמן יש להמתין למנה חסרה, שיפור הדיוק בהערכת ה-RTT יתרום להגדרה נכונה יותר של ערכי פסק זמן (Timeout). מכיון שכך, המארח לא יוכל לבקש שידור חוזר של מנה, עד שעובר פרק הזמן הנחוץ לה. תזמון טוב יותר משפר את הביצועים בקישורי רשת מרוחקים, כגון רשתות מרחביות (WAN) הפרוסות על פני שטח גיאוגרפי גדול, או קישורי לווין או אלחוט.

תמיכה ב- IPSec

IPSec (IP Security) מספק את הפלטפורמה האידיאלית לאבטחת תקשורת אינטראנט ואינטרנט. IPSec יכול לאבטח נתיבים בין שני מחשבים, שני Security Gateways או בין Host לבין Security Gateway. IPSec משולב באופן הדוק עם ניהול מדיניות המערכת של

Windows 2000 Server, כדי לאכוף הצפנה בין המערכות. הלקוחות יכולים לקבל קישור מאובטח בהצפנה, המנוהל על ידי מדיניות קבוצתית - אמצעי אבטחה המגן על מידע המועבר ברשתות תקשורת מחשבים. מכיון ש-IPSec משולב במערכת ההפעלה, קל יותר לנהל ולהגדיר אותו מאשר פתרונות של צד-שלישי.

השירותים הזמינים והנדרשים עבור תעבורה מוגדרים תוך שימוש במדיניות IPSec. מדיניות IPSec ניתנת להגדרה באופן מקומי במחשב, או שניתן להחיל אותה באמצעות המדיניות הקבוצתית (Group Policy) של Windows 2000 תוך שימוש בשירותי Active Directory, כפי שמתואר בתרשים 1.5. כאשר משתמשים ב- Active Directory מזהים המארחים את קיומה של מדיניות בעת תהליך הפעלתם (Startup), מיישמים את המדיניות, ומדי פעם בודקים אם קיימים עבורה עדכונים. מדיניות IPSec מציינת את נושא יחסי האמון (Trust Relationship) שבין המחשבים. יחסי אמון הקלים ביותר לשימוש הם יחסי האמון של Windows 2000 Domain, המבוססים על גירסה 5 של פרוטוקול Kerberos. מדיניות IPSec המוגדרת מראש, מוגדרת לסמוך על מחשבים מאותו Domain, או במחשבים מ- Trusted Windows 2000 Domains אחרים.



תרשים 1.5 מדיניות קבוצתית של Windows 2000 המשתמשת ב- Active Directory

בשכבת ה-IP (שכבת הרשת), מתייחסים לכל מנה יוצאת או נכנסת כאל צרור נתונים (Datagram). כל צרור נתוני IP נושא עליו את כתובת IP של המקור השולח ואת כתובת IP של היעד המקבל. כל צרור נתוני IP מעובד בשכבת ה-IP ומושווה אל מול ערכת מסננים המסופקים על ידי מדיניות האבטחה, אשר מנוהלת על ידי מנהל עבור מחשב, משתמש, קבוצת משתמשים או Domain שלם. שכבת ה-IP יכולה לבצע אחת מהפעולות הבאות על צרור נתונים:

- ❖ לספק שירותי IPSec לצרור הנתונים.
- ❖ לאפשר לצרור הנתונים לעבור, מבלי לשנות בו דבר.
- ❖ להשמיד את צרור הנתונים.

מכיון שבדרך כלל IPSec מצפין את כל מנת ה-IP, לכידת צרור נתוני IPSec שנשלחה לאחר שכבר הושג שיוך אבטחה (**S**ecurity **A**ssociation ,SA), יגלה מעט מאוד מהנתונים הארוזים בצרור הנתונים הזה. החלקים היחידים של המנה שניתן יהיה לנתח את תוכנם, או לקרוא את התוכן על ידי רחרחן רשת (Network Sniffer), כגון Network Monitor, הן כותרות

Ethernet וכותרות IP. דבר זה מאפשר אבטחה טובה יותר לעסקאות IP. פרק 5 דן בהרחבה בנושא IPSec.

איכות שירות כללית

איכות שירות כללית (**G**eneric **Q**uality **o**f **S**ervice ,GQoS) היא שיטה באמצעותה יכולה רשת TCP/IP להציע אחריות לגבי איכות השירות עבור יישומי מולטימדיה. GQoS מאתר רוחבי פס שונים עבור כל חיבור, על בסיס הצרכים.

QoS מאפשר למנהלי רשתות להשתמש במשאבים הקיימים שלהם ביעילות ולהבטיח שיישומים קריטיים יקבלו שירות ברמה גבוהה, מבלי שיצטרכו להגדיל או להרחיב את הרשת הקיימת. ביישום QoS הכוונה שמנהלי רשתות יכולים לשלוט טוב יותר ברשתות שלהם, להפחית הוצאות ולשפר את שביעות רצונו של הלקוח. חבילת רכיבי QoS הנכללת ב-Windows 2000 עובדת עם מנגנון QoS שונה מזה שניתן למצוא ברכיבי רשת, כגון נתבים (Routers) ומתגים (Switches). מנגנונים מארחים אלה נותנים למנהלים להבין איזה יישומים פועלים ומה הן דרישות המשאבים שלהם, מבלי לחשב את המיפויים שבין משתמשים ממשיים, יציאות רשת וכתובות. כאשר המארח והרשת פועלים בכפיפה אחת, ניתן לנצל משאבים בקלות ובחוכמה.

רכיבי QoS הבאים נכללים כיום במערכת ההפעלה Windows 2000 :

- **Application Programming Interface (API) של Generic Quality of Service (GQoS).** ה-API של GQoS הוא ערכת משנה של WinSock 2 API, המאפשר ליישומים להפעיל שירותי QoS ממערכת ההפעלה, מבלי הצורך להבין את המנגנון הפועל מאחוריהם.
- **QoS Service Provider.** רכיב זה מגיב לבקשות המגיעות מה-API של GQoS. הוא מספק איתות RSVP (Resource Reservation Protocol) ותמיכה במדיניות QoS עם Kerberos. הוא גם מפעיל את מנגנון בקרת הזרימה.
- **שירות Admission Control Service (ACS) ופרוטוקול Subnet Bandwidth Manager (SBM).** רכיב זה מספק ניהוליות של משאבים משותפים ברשת על פרוטוקול איתות תקני.
- **תשתית בקרת זרימה.** תשתית זו כוללת מתזמן ומסמן מנות (Packet Scheduler, Marker) לשם בקרת זרימה על מנהלי התקן (drivers) וכרטיסי רשת, להם אין תכונות תזמון וסימון מנות משלהם. היא גם מסמנת מנות עבור dffiserv ועבור 802.1p. בקרת הזרימה של Windows 2000 כוללת מנגנונים נוספים, כגון ISSLOW (**I**ntegrated **S**ervices over **Slow** Links) ו- ATM (**A**synchronouse **T**ransfer **M**ode).

חברת Microsoft עובדת בשיתוף עם חברת Cisco לאספקת שירותי QoS איכותיים, ומשתפת פעולה גם עם Cisco, Extreme Networks, אינטל, Sun, 3Com וחברות נוספות להמשך פיתוח של תקן RSVP, שפיתוחו החל בכוח המשימה IETF (**I**nternet **E**ngineering **T**ask **F**orce).

NWLink

NWLink הוא התואם של Microsoft לפרוטוקול IPX/SPX עבור Windows 2000. NWLink יעיל במקום בו פועלים יישומי שרת/לקוח של NetWare הדורשים שימוש בפרוטוקולים WinSock או NetBIOS over IPX/SPX. WinSock הוא API המאפשר ליישומים מבוססי Windows לגשת לפרוטוקולי התעבורה (Transport Protocols). NWLink יכול להיות פעיל במחשב בו פועלת מערכת ההפעלה Windows 2000 Server או Windows 2000 Professional לצורך גישה לשרתי NetWare.

NWLink בפני עצמו אינו מאפשר למחשב Windows 2000 לגשת לקבצים או למדפסות המשותפים בשרת NetWare, או לשמש כשרת קבצים ו/או הדפסה עבור לקוחות NetWare. כדי לגשת לקבצים או מדפסות בשרת NetWare יש להיעזר במנתב (Redirector), כגון Client Service for NetWare במחשב Windows 2000 Professional, או Gateway Service for NetWare במחשב Windows 2000 Server. NWLink מצורף לכל מהדורות מערכת ההפעלה Windows 2000, והוא מותקן באופן אוטומטי בעת התקנת Client Service for NetWare או Gateway Service for NetWare. הן Client Service for NetWare והן Gateway Service for NetWare מסתמכים על פרוטוקול NWLink. פרק 3 דן בהרחבה בנושא NWLink.

Gateway Service for NetWare

Gateway Service for NetWare עובד עם NWLink כדי לספק גישה לשירותי קבצים, מדפסות ומדריך של NetWare, על ידי כך שהוא פועל כ-gateway דרכו יכולים מספר לקוחות לגשת למשאבי NetWare. באמצעות Gateway Service for NetWare תוכל לחבר מחשב הפועל בסביבת Windows 2000 Server לשרתי NetWare מבוססי-Bindery ולשרתי NDS של נובל. אז, יכולים מספר מרובה של לקוחות מבוססי-Windows להשתמש ב- Gateway Service for NetWare כ- Common Gateway לשם גישה לשירותי קבצים, מדפסות ומדריך של NetWare, מבלי שתידרש תוכנת לקוח ייעודית.

Gateway Service for NetWare תומך בגישה ישירה לשירותי NetWare ממחשב הפועל בסביבת Windows 2000 Server באופן דומה לזה בו Client Service for NetWare תומך בגישה ישירה ממחשב לקוח. בנוסף, Gateway Service for NetWare תומך גם בתסריטי כניסה של NetWare.

הערה Gateway Service for NetWare **כלול** רק בגרסאות Windows 2000 Server ו- Windows 2000 Advanced Server.

Client Service for NetWare

בדומה ל- Gateway Service for NetWare, Client Service for NetWare עובד עם NWLink כדי לספק גישה לשירותי קבצים, מדפסות ומדריך של NetWare. אבל, במקום לפעול כ-gateway עבור הלקוחות, Client Service for NetWare מאפשר ללקוחות להתחבר ישירות לשירותי הקבצים והמדפסות שבשרתי NetWare מבוססי-Bindery ובשרתי NetWare המפעילים NDS. Client Service for NetWare תומך גם הוא בתסריטי התחברות של NetWare. Client Service for NetWare כלול רק ב- Windows 2000 Professional.

NetBEUI

NetBEUI (**NetB**IOS **E**nhanced **U**ser **I**nterface) פותח במקורו כפרוטוקול עבור רשתות LAN קטנות, של בין 20 ועד 200 מחשבים. NetBEUI אינו בר-ניתוב, מפני שהוא חסר את שכבת הרשת (Network Layer). NetBEUI כלול ב- Windows 2000 Server וב-Windows 2000 Professional. הוא כלול בהן מטעמי תאימות לאחור בלבד, כדי לתמוך בתחנות עבודה שלא שודרגו למערכת ההפעלה Windows 2000.

AppleTalk

AppleTalk הוא חבילת פרוטוקולים שפותחה על ידי Apple Computers לשם תקשורת בין מחשבי מקינטוש. Windows 2000 כוללת תמיכה ב-AppleTalk, מה שמאפשר ל-Windows 2000 לתפקד כנתב (Router) ושרת חיוג (Dial-up Server). התמיכה מסופקת במקורה כשירות לשיתוף קבצים ומדפסות.

Windows 2000 תומכת במחסנית פרוטוקול (Protocol Stack) AppleTalk ובתוכנת ניתוב של AppleTalk, כך ששרת Windows 2000 יכול להתחבר אל ולספק שירותי ניתוב עבור רשתות מקינטוש, מבוססות-AppleTalk.

Data Link Control

Data **L**ink **C**ontrol (DLC) פותח במקורו עבור תקשורת Mainframe של יבמ. פרוטוקול זה לא נועד להיות פרוטוקול עיקרי לשימוש בין מחשבים אישיים. השימוש האחר ב-DLC הוא לשם הדפסה להתקני הדפסה מתוצרת Hewlett-Packard המחוברים ישירות לרשת. מדפסות מחוברות לרשת משתמשות בפרוטוקול DLC, מפני שהמסגרות (Frames) המתקבלות ניתנות לפירוק בקלות, וניתן לתכנת בקלות יתרה את פונקציונליות DLC לרכיבי ה-ROM (זיכרון לקריאה בלבד) של המדפסות. יעילותו של DLC מוגבלת, מפני שאין לו ממשק ישיר לשכבת ממשק מנהל התקן התעבורה (Transport Driver Interface Layer). יש להתקין את DLC רק במחשבי הרשת המבצעים את שתי הפעולות הללו, כגון שרת הדפסה השולח נתונים להתקן הדפסה (printer driver) ברשת מתוצרת Hewlett-Packard. לקוחות השולחים עבודות הדפסה למדפסת רשת אינם צריכים שפרוטוקול DLC יהיה מותקן בהם. רק שרת ההדפסה המתקשר באופן ישיר עם התקן (Driver) ההדפסה צריך שיהיה מותקן בו DLC (במדפסות HP החדישות אין צורך להשתמש ב-DLC).

Infrared Data Association

Infra**r**ed **D**ata **A**ssociation (IrDA) מגדיר קבוצה של פרוטוקולים אינפרה-אדום, אלחוטי דו-כיווני, מהיר ולטווח קצר, אליהם מתייחסים בדרך כלל כאל IrDA. IrDA מאפשר למיגוון התקנים לתקשר האחד עם השני. מצלמות, מדפסות, מחשבים ניידים, מחשבים שולחניים ומחשבי כף-יד (מוכרים באנגלית בשם Personal Digital Assistants, ובקיצור PDA), יכולים לתקשר עם התקנים תואמים באמצעות טכנולוגיה זו.

סיכום שיעור

TCP/IP הוא חבילת פרוטוקולים המוגדרים כתקן תעשייתי (Industry Standard), שנועדה לשימוש ברשתות גדולות. זהו פרוטוקול בר-ניתוב, מה שאומר שניתן למתג (Switch) מנות נתונים תוך שימוש בכתובת היעד של המנה. יכולתו של TCP/IP להיות מנותב מספקת Fault Tolerance. פרוטוקולים אחרים הנתמכים על ידי Windows 2000 כוללים:

- NWLink
- NetBEUI
- AppleTalk
- **D**ata **L**ink **C**ontrol (DLC)
- **I**nfra**r**ed **D**ata **A**ssociation (IrDA)

שאלות סיכום

השאלות הבאות נועדו לחזק את הנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות לשאלה, עיין בשיעור המתאים ונסה את השאלה שנית. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך מופיעות השאלות באנגלית ולאחר מכן בעברית.

Answering the following questions will reinforce key information presented in this chapter. Answers to the questions can be found in Appendix A, "Questions and Answers".

1. You are currently configuring TCP/IP manually for new computers and computers moving from one subnet to another. You want to simplify management of TCP/IP addresses and assign them automatically. Which Windows 2000 network service should you use?
2. You have an Alpha server with 8GB or RAM and 8 CPUs. You want to provide file services to over 400 people in your company. Which Windows 2000 operating system would be most appropriate to deploy, and why?
3. You want a Windows 2000 server to connect to and provide routing for AppleTalk-based Macintosh networks. What protocol should you install?

1. נכון להיום אתה מגדיר באופן ידני את תצורת TCP/IP במחשבים חדשים ובמחשבים העוברים מ-Subnet אחת לאחרת. אתה מעוניין לפשט את ניהול כתובות TCP/IP ולהקצות אותן באופן אוטומטי. באיזה שירות רשת של Windows 2000 עליך להשתמש?
2. יש לך שרת מבוסס מעבד Alpha ובו 8GB זיכרון RAM ושמונה מעבדים. אתה מעוניין לספק שירותי קבצים ליותר מ-400 עובדים בארגון. איזו מהדורה של מערכת ההפעלה Windows 2000 יהיה נכון ביותר להטמיע, ומדוע?
3. אתה מעוניין בשרת Windows 2000 אליו ניתן להתחבר ואשר יספק שירותי ניתוב עבור רשתות מקינטוש מבוססות-AppleTalk. איזה פרוטוקול עליך להתקין?

פרק 2

יישום TCP/IP

אודות פרק זה

בפרק זה נסקור את TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol). השיעורים בפרק זה מתארים בקצרה את ההיסטוריה של TCP/IP, דנים בתהליך תקינת האינטרנט וסוקרים תוכניות שירות ל-TCP/IP. תלמד כיצד לשייך כתובות IP למספר מרובה של רשתות TCP/IP בעלות מזהה רשת (Network Identifier) יחיד. השיעורים מתארים את התפיסות הבסיסיות ואת התהליכים ליישום רשתות משנה (Subnet) ורשתות על (Supernet). במהלך השיעורים תלמד מתי נדרשת רשת משנה, כיצד ומתי להשתמש במסכת רשת משנה של ברירת מחדל (Default Subnet Mask), כיצד להגדיר מסכת רשת משנית מותאמת באופן אישי (Custom Subnet Mask) וכיצד ליצור מרחב כתובות IP חוקיות עבור כל רשת משנה.

לפני שתתחיל

להשלמת פרק זה צריך שיהיה ברשותך :

- שרת Windows 2000 מותקן ופעיל.

שיעור 1: סקירת TCP/IP

TCP/IP ‏(**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) הוא חבילת פרוטוקולים הנחשבת לתקן תעשייתי שנועד עבור רשתות רחבות (WAN). ‏Windows 2000 תומכת בהרחבה ב-TCP/IP, הן כחבילת פרוטוקולים והן כערכת שירותים להתחברות ולניהול רשתות מבוססות IP. שיעור זה כולל סקירה של תפיסות TCP/IP, מונחים מקצועיים (טרמינולוגיה) ומתאר כיצד נוצרו תקני האינטרנט. בנוסף תלמד בשיעור זה כיצד משולב TCP/IP במערכת ההפעלה Windows 2000.

לאחר שיעור זה, תוכל

- להגדיר את TCP/IP ולתאר את יתרונותיו בסביבת Windows 2000.
- להגדיר כיצד ניתן למפות את חבילת הפרוטוקולים TCP/IP למודל בן ארבע שכבות.
- לתאר כיצד TCP ‏(**T**ransmission **C**ontrol **P**rotocol) ו- UDP ‏(**U**ser **D**atagram **P**rotocol) מעבירים נתונים.

זמן לימוד משוער: 45 דקות

יתרונות TCP/IP

כל מערכות ההפעלה המודרניות מציעות תמיכה ב-TCP/IP, ורוב הרשתות הגדולות סומכות על TCP/IP עבור רוב תעבורת הרשת שלהן. TCP/IP הוא גם הפרוטוקול התקני של רשת האינטרנט. מעבר לכך, תוכניות שירות תקניות רבות משתמשות בפרוטוקול זה. חלק מאותן תוכניות שירות נפוצות, כגון FTP ‏(**F**ile **T**ransfer **P**rotocol) או Telnet, נכללות במערכת ההפעלה Windows 2000 Server. ניתן לשלב בקלות רשתות מבוססות TCP/IP עם האינטרנט. בשל הפופולריות הרבה לה הוא זוכה, TCP/IP גם זוכה לפיתוחים רבים ומציע מיגוון רחב מאוד של תוכניות שירות המשפרות את תפקודיו, ביצועיו ואבטחתו. רשתות המבוססות על פרוטוקולי תעבורה (Transport Protocol) אחרים, כגון ATM או AppleTalk, יכולות להשתלב בקלות יתרה עם רשתות מבוססות TCP/IP, באמצעות התקן הידוע בשם Gateway. על ידי הוספת TCP/IP לתצורת Windows 2000 עומדים לפניך היתרונות הבאים:

- טכנולוגיה לקישור בין רשתות שונות. TCP/IP הוא פרוטוקול בר-ניתוב ויכול לתקשר עם רשתות שונות באמצעות Gateways.
- אפשרות למסגרת עבודה יציבה, המאפשרת שינויים בגודלה וחוצת-פלטפורמה ליישומי שרת/לקוח. TCP/IP של Microsoft מציע ממשק WinSock, שהוא אידיאלי לפיתוח יישומי שרת/לקוח, אותם ניתן להפעיל במחסנית תואמת-WinSock ‏(WinSock-Compliant Stack) של יצרנים אחרים.
- שיטה ליצירת גישה לרשת האינטרנט. על ידי חיבור לאינטרנט ניתן ליצור רשת פרטית וירטואלית (**V**irtual **P**rivate **N**etwork, VPN) או אקסטראנט (Extranet), דבר המאפשר גישה מרחוק שאינה יקרה.

בנוסף לכך, לקוחות מקינטוש יכולים להיעזר בפרוטוקול TCP/IP לשם גישה לשיתופי רשת (Shares) בשרת Windows 2000 המפעיל את שירותי הקבצים עבור מקינטוש (AFT [AppleShare File Server] over IP), מה שמקל על רישות עם מחשבי מקינטוש.

פרוטוקלי התקשורת TCP/IP של Windows 2000

תכונה משמעותית של Windows 2000 היא היכולת להתחבר לאינטרנט ולמערכות שונות. Windows 2000 גם כוללת תכונות אבטחה משופרות אותן ניתן להחיל כאשר מחברים מערכת ברשת. כדי לתמוך בכל התכונות הללו יש ל-TCP/IP של Microsoft יכולות חדשות ומורחבות. ביניהן:

- ❖ **IP Security.** ‏**IP Sec**urity ‏(IPSec) היא טכנולוגיה המשמשת להצפנת תעבורת רשת TCP/IP. ‏IPSec מאפשר אבטחת נתונים בין לקוחות מרוחקים ושרתים פרטיים בארגון באמצעות VPN ‏(Virtual Private Network).
- ❖ **Point-to-Point Tunneling Protocol.** פרוטוקול תיעול מנקודה-לנקודה (PPTP) המאפשר יצירת VPN דרך האינטרנט, בדומה לזו של IPSec. ‏PPTP גם תומך במיגוון רחב של פרוטוקולים, כגון IP, ‏IPX ‏(Internetwork Packet Exchange) ו- NetBEUI ‏(**NetB**IOS **E**nhanced **U**ser **I**nterface).
- ❖ **Layer Two Tunneling Protocol.** פרוטוקול L2PT הוא שילוב של PPTP עם L2F ‏(**L**ayer **Two** **F**orwarding). ‏L2F הוא פרוטוקול תעבורה המאפשר לשרתי גישה בחיוג למסגר (Frame) תעבורת חיוג (Dial-up) ב-PPP, ולשדר אותה דרך קישורי WAN לשרת L2F ‏(נתב, Router).

לבסוף, Microsoft ממשיכה לתמוך במערכות מיושנות (Legacy Systems) ובפרוטוקולים מיושנים כדי לשמר את השקעות העבר של לקוחותיה ולהפחית את הסיכון, הלחץ והמעמסה הכלכלית שבניהול סביבות הטרוגניות. מסיבה זו תומכת Windows 2000 ב:

- ❖ AppleTalk
- ❖ IPX/SPX ‏(**I**nternetwork **P**acket E**x**change/**S**equenced **P**acket E**x**change)
- ❖ NetBEUI

פרוטוקולים אלה מסייעים לשמירה על סביבות הטרוגניות ומאפשרות הגירה לפלטפורמת TCP/IP עשירה יותר וגמישה יותר המבוססת על Windows 2000.

הרחבות TCP/IP Stack

Windows 2000 כוללת מספר הרחבות ל-TCP/IP, וביניהן:

- ❖ תמיכה בחלון גדול, המשפרת ביצועים כאשר מנות רבות נמצאות במעבר למשך זמן רב.
- ❖ אישורי קבלה ברירניים (Selective Acknowledgments) המאפשרים למערכת להתאושש במהירות ממצב יתירות (Congestion). על השולח לשלוח מחדש רק את אותן מנות שלא התקבלו.
- ❖ אפשרות להערכה טובה יותר של משך הזמן הלוך-ושוב (Round-Trip) של מנה.
- ❖ אפשרות לקביעה טובה יותר של עדיפויות תעבורה, עבור יישומים הדורשים זאת.

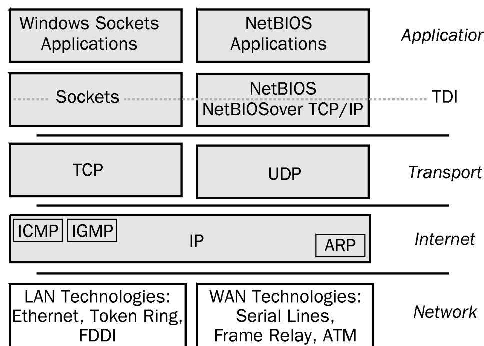
תוכניות שירות של TCP/IP

תוכניות השירות של TCP/IP הכלולות ב- Windows 2000 כוללות, בין השאר:

- **תוכניות שירות להעברת נתונים.** Windows 2000 כוללת תמיכה למספר פרוטוקולי תעבורה מבוססי IP שונים. אלו כוללים את פרוטוקול העברת הקבצים FTP (**F**ile **T**ransfer **P**rotocol), HTTP (**H**yper**T**ext **T**ransfer **P**rotocol) ואת CIFS (**C**ommon **I**nternet **F**ile **S**ystem).
- **Telnet.** למארחי UNIX יש היסטוריה של ניהול באמצעות Telnet. זהו ממשק טקסטואלי, הדומה למנחה שורת פקודה, אליו ניתן לגשת ברשת IP. Windows 2000 כוללת גם לקוח וגם שרת Telnet.
- **תוכניות שירות להדפסה.** Windows 2000 מסוגלת להדפיס ישירות למדפסות מבוססות-IP, דהיינו להדפיס לכתובת URL. מעבר לכך, שתי תוכניות שירות של TCP/IP מאפשרות להדפיס ולקבל תמונת מצב הדפסה במדפסת TCP/IP. LPR (**L**ine **P**rinter) (**R**emote) מדפיס קובץ למארח, בו פועל שירות LPD (**L**ine **P**rinter **D**aemon). LPQ (**L**ine **P**rinter **Q**ueue) מציג את מצב תור ההדפסה במארח, בו פועל שירות LPD.
- **תוכניות שירות לאבחון.** Windows 2000 כוללת מספר תוכניות שירות אשר ייעודן הוא אבחון בעיות מבוססות-TCP/IP. ביניהן: PING, Ipconfig, Nslookup ו- Tracert.

סקירת ארכיטקטורת חבילת הפרוטוקולים TCP/IP

פרוטוקולי TCP/IP מספקים תמיכה ברישות לשם חיבור כל המארחים והאתרים, וכדי לעמוד בתקנים לאופן בו מתקשרים מחשבים ורשתות. פרוטוקולי TCP/IP בנויים על מודל ארבע-שכבות, הידוע בשם מודל משרד ההגנה (DOD, **D**epartment **O**f **D**efence model): יישום (Application), תעבורה (Transport), אינטרנט (Internet) וממשק הרשת (Network Interface), כפי שניתן לראות בתרשים 2.1.



תרשים 2.1 מודל ארבע השכבות של TCP/IP

שכבת היישום (Application)

שכבת היישום עומדת בראש מודל ארבע השכבות של TCP/IP, והיא המקום בו התוכנה מקבלת את הגישה לרשת. שכבה זו מקבילה לשכבות Session, Presentation ו- Application של מודל OSI, בן שבע השכבות.

השירותים ותוכניות השירות כוללות:

- **HTTP ‏(HyperText Transfer Protocol).** פרוטוקול זה משמש את רובה המכריע של קהילת ה-WWW ‏(World Wide Web) באינטרנט. Windows 2000 כוללת את הדפדפן Internet Explorer כלקוח HTTP ואת IIS ‏(**I**nternet **I**nformation **S**erver) כשרת HTTP.
- **FTP ‏(File Transfer Protocol).** FTP הוא שירות אינטרנט שנועד להעברת קבצים ממחשב אחד לאחר. Internet Explorer ותוכנית שורת הפקודה FTP שניהם מתפקדים כלקוחות FTP. IIS כולל גם שרת FTP.
- **SMTP ‏(Simple Mail Transfer Protocol).** בפרוטוקול זה משתמשים שרתי דואר אלקטרוני להעברת הודעות. IIS יכול לשלוח הודעות תוך שימוש בפרוטוקול זה.
- **Telnet.** פרוטוקול הדמיית מסוף (Terminal Emulation Protocol) היכול לשמש לצרכי כניסה למארחים מרוחקים (Remote Hosts). Telnet מציע למשתמשים בו את האפשרות להפעיל תוכניות באופן מרוחק ומקל על ניהול מרחוק. Telnet זמין בעיקרון לכל מערכות ההפעלה ומקל על השילוב בין סביבות רישות הטרוגניות. Windows 2000 כוללת הן שרת והן לקוח עבור Telnet. Telnet משמש בעיקר במערכות מבוססות UNIX.
- **DNS ‏(Domain Name System).** DNS הוא ערכת פרוטוקולים ושירותים ברשת TCP/IP המאפשרת למשתמשי הרשת להשתמש בשמות היררכיים ידידותיים לאיתור והתחברות למארחים, במקום שיצטרכו לזכור ולהשתמש בכתובות IP שלהם. ברחבי האינטרנט וברשתות של ארגונים גדולים נעשה כיום שימוש נרחב ב-DNS. כאשר אתה משתמש בדפדפן אינטרנט, יישום Telnet, תוכנית FTP או תוכנית שירות אחרת של TCP/IP באינטרנט, רוב הסיכויים שאתה משתמש ב-DNS. Windows 2000 כוללת גם שרת DNS.
- **SNMP ‏(Simple Network Management Protocol).** פרוטוקול זה מאפשר לנהל רכיבים (Nodes) ברשת, כגון שרתים, תחנות עבודה, נתבים, גשרים ורכזות ממארח מרכזי אחד. ניתן להשתמש ב-SNMP גם להגדרת התקנים מרוחקים, ניטור ביצועי הרשת, זיהוי תקלות ברשת או גישה לא חוקית ולבקר (Audit) את השימוש ברשת.

ממשקי תכנות יישומים של יישומי רשת

TCP/IP מספק ליישומי הרשת שני ממשקים בהם יוכלו להשתמש בשירותי מחסנית פרוטוקול TCP/IP:

- **WinSock.** היישום של Windows 2000 לממשקי תכנות היישומים (API) של Sockets, בהם נעשה שימוש נרחב. API של Sockets הוא המנגנון התקני לגישה לשירותי צרור נתונים ו- Session באמצעות TCP/IP ‏(Datagram / Session over TCP/IP).
- **NetBIOS.** API תקני המשמש כמנגנון תקשורת פנימי (IPC, **I**nter-**P**rocessing **C**ommunication) בסביבת Windows. למרות ש-NetBIOS יכול לשמש לשם התחברות תקנית לפרוטוקולים התומכים בשירותי מתן השמות וההודעות של NetBIOS, כגון TCP/IP או NetBEUI, הוא נכלל ב-Windows 2000 בעיקר כדי לתמוך ביישומים מיושנים.

שכבת התעבורה (Transport)

פרוטוקולי תעבורה מספקים את Sessions ההתקשרות בין מחשבים ומגדירים את סוג שירות התעבורה כ- Connection-Oriented (TCP) או כ- Connectionless Datagram-Oriented (UDP). TCP מספק תקשורת Connection-Oriented אמינה עבור יישומים שבדרך כלל מעבירים כמויות גדולות של נתונים בכל רגע נתון. הוא גם משמש יישומים הדורשים אישור על קבלת הנתונים. מצד שני, UDP מספק תקשורת Connectionless, ואינו מבטיח את משלוח המנות. יישומים המשתמשי ב-UDP מעבירים, בדרך כלל, כמויות קטנות של נתונים בכל רגע נתון. שלמות העברת הנתונים היא באחריותו של היישום עצמו. שכבת התעבורה במודל DOD היא המקבילה לשכבה Transport במודל OSI. UDP משמש, בדרך כלל, להעברת שידורי Video/Audio ברשת האינטרנט.

שכבת האינטרנט (Internet)

פרוטוקולי אינטרנט אורזים את המנות ליצירת צרורות נתונים (Datagrams) ומפעילים את כל אלגוריתמי הניתוב הנדרשים. פעילויות הניתוב אותן מבצעת שכבת האינטרנט נדרשים כדי לאפשר למארחים לפעול יחד עם רשתות אחרות. שכבת האינטרנט היא המקבילה לשכבת הרשת (Network Layer) של מודל OSI. בשכבה זו מיושמים חמישה פרוטוקולים:

- ARP (**A**ddress **R**esolution **P**rotocol), הקובע את כתובת החומרה של המארחים.
- RARP (**R**everse **A**ddress **R**esolution **P**rotocol), אשר מספק הסדרת כתובת הפוכה במארח המקבל (למרות ש-Microsoft אינה מיישמת את פרוטוקול RARP, ניתן למצוא אותו במערכות של יצרנים אחרים, והוא מוזכר כאן לשם השלמת החומר).
- ICMP (**I**nternet **C**ontrol **M**essage **P**rotocol) השולח הודעות שגיאה ל-IP כאשר כזו מתרחשת.
- IGMP (**I**nternet **G**roup **M**anagement **P**rotocol) אשר מיידע נתבים אודות זמינותם של חברים בקבוצות Multicast.
- IP (**I**nternet **P**rotocol) אשר ממען ומנתב את המנות.

שכבת ממשק הרשת (Network Interface)

בבסיסו של המודל נמצאת שכבת ממשק הרשת (Network Interface). לכל אחת מהרשתות המקומיות (LAN), הרשתות העירוניות (MAN), רשתות מרחביות (WAN), ומסוגי החיוג (Dial-up) כגון Ethernet, Token Ring, FDDI (**F**iber **D**istributed **D**ata **I**nterface) ו-ARCnet, יש דרישות אחרות בכל הנוגע לכבילה (חיווט), איתות וקידוד נתונים. שכבת ממשק הרשת מציינת את הדרישות המקבילות לשכבות קישור הנתונים (Data Link) והפיסית (Physical) של מודל OSI. שכבת ממשק הרשת אחראית לשליחת ולקבלת מסגרות (Frames), שהן מנות נתונים המועברות ברשת כיחידה אחת. שכבת ממשק הרשת היא המניחה את המסגרות ברשת וגם מושכת אותן מהרשת.

טכנולוגיות TCP/IP ב-WAN

קיימות שתי טכנולוגיות WAN עיקריות הנתמכות על ידי TCP/IP :

1. קווים טוריים (Serial Lines) הכוללים חיוג אנלוגי, קווים דיגיטליים וקווי נל״נ.

   בדרך כלל מועבר TCP/IP בקווים טוריים תוך שימוש בפרוטוקול SLIP (**S**erial **L**ine **I**nternet **P**rotocol) או פרוטוקול PPP (**P**oint-to-**P**oint **P**rotocol). Windows 2000 Server תומך בשני הפרוטוקולים באמצעות RRAS (**R**outing and **R**emote **A**ccess **S**ervice). מכיון שרמת האבטחה האפשרית בעת השימוש ב-PPP גבוהה יותר, אפשרויות ההגדרה שלו נוחות יותר והוא מאפשר זיהוי שגיאות, שלא כמו SLIP, זהו הפרוטוקול המומלץ לשימוש בעת העבודה עם קווים טוריים.

2. רשתות מיתוג-מנות (Packet-Switched Networks), הכוללות X.25, ממסור מסגרות (Frame Relay) ו-ATM (Asyncronous Transfer Mode).

הערה Windows 2000 **תומכת רק בפונקציונליות הלקוח של** SLIP**, לא בזו של השרת.** RRAS **של** Windows 2000 **אינו מקבל חיבורי לקוחות** SLIP.

TCP - Transmission Control Protocol

TCP הוא שירות שילוח Connection-Oriented אמין. נתוני TCP נשלחים במקטעים (Segment), ועל המארחים להקים ביניהם Session לפני שניתן להעביר ביניהם נתונים. TCP משתמשת בתקשורת שטף-בתים (Byte-Stream), מה שאומר שהנתונים מטופלים כסדרה של בתים.

אמינותו של TCP מושגת על ידי שיוך מספר סדרה (Sequence Number) לכל מקטע המועבר. אם מקטע כלשהו מתחלק לחלקים קטנים יותר, יודע הצד המקבל אם כל החלקים התקבלו. אישור (Acknowledgment) מוודא שהצד המקבל אכן קיבל את הנתונים. עבור כל מקטע שנשלח חייב הצד המקבל להחזיר אישור (ACK) בתוך פרק זמן מסוים. אם השולח אינו מקבל את האישור (ACK), אז נשלחים הנתונים פעם נוספת. אם מקטע כלשהו הגיע ליעדו כשהוא פגום, הצד המקבל משמיט אותו ומתעלם ממנו. מכיון שבמקרה כגון זה לא יישלח אות אישור, השולח ישדר מקטע זה פעם נוספת.

IP - Internet Protocol

למרות ש-TCP מפריד נתונים למנות חסויות והוא גם זה שאחראי להבטחת המשלוח שלהן, IP הוא זה המבצע את המשלוח בפועל. בשכבת פרוטוקול האינטרנט (IP Layer), מתייחסים לכל מנה, נכנסת או יוצאת, כאל צרור נתונים (Datagram). שדות צרורות הנתונים של IP בטבלה הבאה נוספים לכותרת, כאשר המנה מועברת כלפי מעלה משכבת ממשק הרשת (Network Interface Layer).

שדה	פעולה
Source IP Address	מזהה את שולח צרורות הנתונים על פי כתובת IP.
Destination IP Address	מזהה את יעדו של צרור הנתונים, על פי כתובת IP.
Protocol	מודיע ל-IP במארח היעד אם להעביר את המנה כלפי מעלה ל-TCP או ל-UDP.
Checksum	חישוב מתמטי פשוט המשמש לוודא את שלמות המנות עם הגעתן.
TTL (**T**ime **t**o **L**ive)	מציין את מספר השניות בהן מותר לצרור נתונים "לבלות" במעבר, לפני שהוא יושמט. בדרך זו נמנע ממנות להסתובב בלולאה אין-סופית ברשת. כל נתב (Router) המעביר את המנה מפחית את ערך TTL באחד. ערך ברירת המחדל של TTL לסביבת Windows 2000 הוא 128 שניות.

UDP - User Datagram Protocol

UDP מציע שירות צרורות נתונים Connectionless Datagram Service שאינו מבטיח את שליחת הנתונים, וגם לא את סדר המשלוח. סכומי הביקורת (Checksums) של נתוני UDP הם אופציונליים, ומספקים דרך לחילופי נתונים ברשתות בעלות אמינות גבוהה, מבלי לגזול משאבי רשת יקרים, או זמן עיבוד. השימוש ב-UDP הוא בידי יישומים שאינם דורשים אישור על קבלת נתונים. בדרך כלל, מעבירים יישומים כגון אלה כמויות קטנות של נתונים בכל רגע נתון. Broadcast Packet חייבות להשתמש ב-UDP. דוגמאות לשירותים ולישומים העובדים עם UDP הן DNS, RIP ו-SNMP.

סיכום שיעור

TCP/IP הוא חבילת פרוטוקולים הנחשבת לתקן תעשייתי, אשר יועדה עבור רשתות מרחביות (WAN). הוספת TCP/IP לתצורת Windows 2000 מציעה מספר יתרונות, וביניהן אמינות, אפשרויות גידול, אבטחה והיכולות לעבוד עם מערכות שונות. Windows 2000 כוללת מספר תוכניות שירות אשר יסייעו לך להתחבר למארחים מבוססי-TCP/IP אחרים, או לפתור תקלות הקשורות בהתחברויות TCP/IP.

פרוטוקולי TCP/IP משתמשים במודל של ארבע שכבות: יישום (Application), תעבורה (Transport), אינטרנט (Internet) וממשק רשת (Network Interface). IP פועל ברמת האינטרנט ותומך בכל ממשקי טכנולוגיות LAN או WAN, כגון Ethernet, Token Ring, Frame Relay ו-ATM. IP הוא פרוטוקול חסר-חיבור הממען ומנתב מנות בין מארחים. IP אינו אמין, מפני שהמשלוח באמצעותו אינו מובטח.

בשכבת התעבורה, TCP מספק IP עם משלוח אמין ו- Connection-Oriented. מרגע שנוצר Session, מעביר TCP את הנתונים ליישומים דרך מספרי יציאות ייחודיים. UDP, פרוטוקול תעבורה חליפי ל-TCP, הוא שירות צרורות נתונים Connectionless Datagram Service, שאינו מבטיח את שליחת הנתונים. השימוש ב-UDP הוא בידי יישומים שאינם דורשים אישור על קבלת נתונים.

שיעור 2: מיעון פרוטוקול אינטרנט

לכל רכיב רשת או מארח המתקשר באמצעות TCP/IP נדרשת כתובת IP ייחודית. ניתן לסווג רשתות TCP/IP לשלוש מחלקות עיקריות להן גדלים מוגדרים מראש. כל רשת יכולה להיות מחולקת לרשתות משנה קטנות יותר על ידי מנהל הרשת, וזאת על ידי השימוש ב-Subnet Mask להפרדת כתובת ה-IP לשני חלקים. חלק אחד מזהה את המארח (מחשב) ואילו החלק השני מזהה את הרשת אליה הוא שייך. כל מארח TCP/IP מזוהה על ידי כתובת IP לוגית. כתובת ה-IP היא כתובת בשכבת הרשת (Network Layer) והיא אינה תלויה בכתובת משכבת קישור הנתונים (Data-Link Layer), כגון כתובת בקרת גישת המדיה של כרטיס ממשק הרשת. בשיעור זה תלמד כיצד פועל מיעון כתובות IP ברשת TCP/IP.

לאחר שיעור זה, תוכל

- לתאר את מטרת כתובת ה-IP.
- להמיר כתובות IP מפורמט בינרי לדצימלי (עשרוני).
- לזהות מחלקות שונות של כתובות IP.

זמן לימוד משוער: 30 דקות

כתובת IP

כתובת IP היא מספר בן 32 סיביות (32-bit) המזהה באופן ייחודי מארח (מחשב או התקן אחר, כגון מדפסת או נתב) ברשת TCP/IP. כתובות IP מבוטאות בדרך כלל במבנה עשרוני מנוקד, כאשר ארבעה מספרים מופרדים באמצעות נקודות, כגון 192.168.123.132.

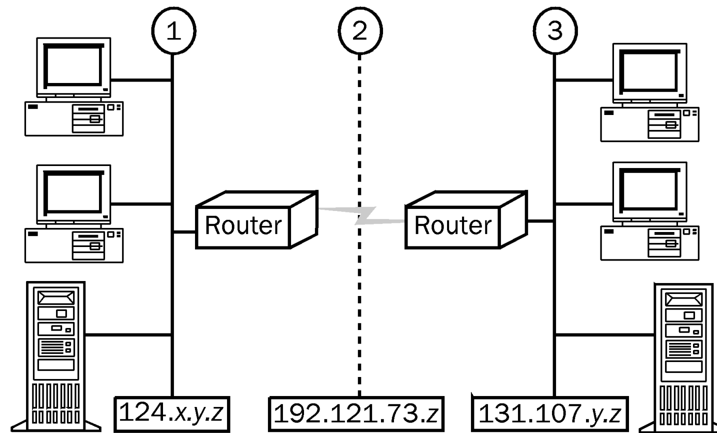
כדי שרשת מרחבית (WAN) תפעל בסביבת TCP/IP ביעילות כאוסף של רשתות, הנתבים (Routers) המעבירים את מנות הנתונים (Packets) בין הרשתות אינם צריכים לדעת את מיקומו המדויק של המארח אליו מיועדת מנת הנתונים. הנתבים יודעים רק באיזו רשת חבר אותו מארח, ומשתמשים במידע האגור בטבלאות הניתוב שלהם כדי לקבוע כיצד להעביר את המנה לרשת מארח היעד. לאחר שהמנה נשלחת לרשת היעד, היא מועברת למארח המתאים. כדי שתהליך זה יצליח יש לכתובת IP שני חלקים: מזהה רשת (Network ID) ומזהה מארח (Host ID).

מזהה הרשת

מזהה הרשת (Network ID) מזהה מארחי TCP/IP הממוקמים באותה רשת פיסית. כדי שהמארחים יוכלו לתקשר ביניהם, יש לשייך את אותו מזהה רשת לכל המארחים באותה רשת פיסית. אם לרשת שלך מחוברים נתבים, כפי שמוצג בתרשים 2.2, יש לשייך לכל חיבור רחב (Wide Area Connection) מזהה רשת ייחודי. לדוגמה, בתרשים הבא:

- Network 2 ו- Network 3 מייצגים שתי רשתות מנותבות.
- Network 2 מייצג חיבור WAN בין הנתבים.

❖ Network 1-3 דורש מזהה רשת, כדי שניתן יהיה לשייך מזהי מארח ייחודיים לשני הממשקים שבין שני הנתבים.

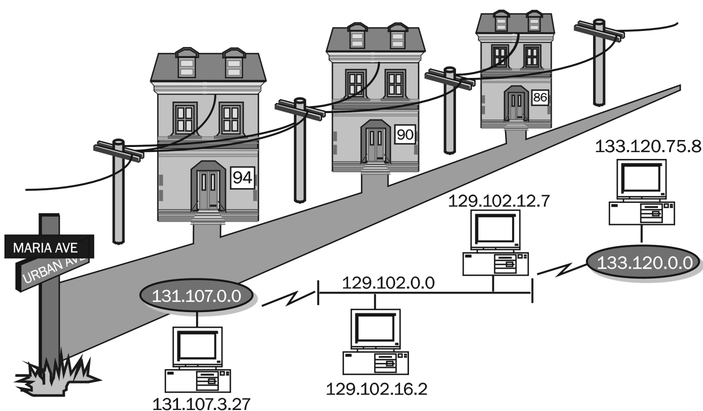


תרשים 2.2 נתבים המחברים בין רשתות

הערה אם אתה מתכנן לחבר את הרשת שלך לאינטרנט, עליך לרכוש את חלק מזהה הרשת של כתובת ה-IP. דבר זה יבטיח לך את ייחודיות מזהה הרשת. לרישום שמות domain (Domain Name Registration) והקצאת מספר רשת IP, פנה לספק שירותי האינטרנט שלך.

מזהה המארח

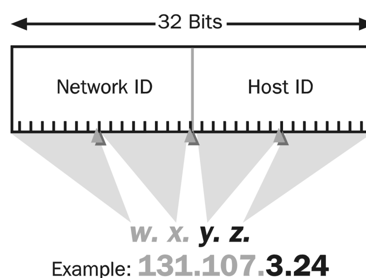
מזהה המארח (Host ID) מזהה מארח בתוך הרשת. מזהה המארח חייב להיות ייחודי לרשת המזוהה על ידי מזהה הרשת. כתובת IP מזהה את מיקום המערכת ברשת, באופן דומה לזה בו מזהה כתובת רחוב בית מסויים בעיר, כפי שמוצג בתרשים 2.3.



תרשים 2.3 מארחים ורכיבי רשת מתקשרים באמצעות TCP/IP

ציון עשרוני מנוקד

קיימים שני פורמטים בהם ניתן להתייחס לכתובת IP - בינרי וציון עשרוני מנוקד (Dotted Decimal Notation). כפי שניתן לראות בתרשים 2.4, כל כתובת IP היא באורך 32 סיביות ומכילה ארבעה מקטעים בני שמונה סיביות כל אחד. מקטעים אלה של שמונה סיביות מוכרים יותר בשם אוקטט (Octet). כתובת IP שהובאה כאן לדוגמה תיראה כך 11000000.10101000.01111011.10000100, כאשר תוסב לפורמט בינרי. המספרים העשרוניים המופרדים באמצעות נקודות בציון העשרוני המנוקד הם האוקטטים שהומרו מפורמט בינרי לפורמט עשרוני מנוקד. האוקטטים מייצגים מספר עשרוני שבין אפס ו-255, וכל 32 הסיביות של כתובת ה-IP מוקצות למזהי הרשת והמארחת, כפי שמוצג בתרשים 2.4.

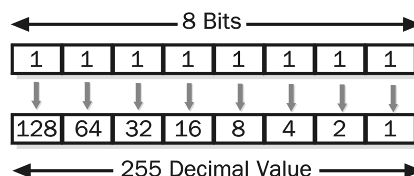


תרשים 2.4 כיצד בנויה כתובת IP

הערה מזהה הרשת אינו יכול לקבל את הערך 127 באוקטט הראשון. מזהה זה שמור לצרכי הלולאה הפנימית (Loopback) ולצרכי אבחון.

המרת כתובת IP מבינרית לעשרונית

כדי לנהל TCP/IP ברשת שלך, עליך לדעת כיצד להמיר ערכי סיבית באוקטט מקוד בינרי לפורמט דצימלי. בפורמט בינרי, לכל סיבית באוקטט יש ערך עשרוני משויך. סיבית לה הערך 0 תהיה תמיד בערך אפס, ואילו סיבית לה הערך 1 יכולה להיות מומרת לערך עשרוני. הסיבית הימנית (הנמוכה מבחינת סדר הסיביות) מייצגת את הערך העשרוני אחד. הסיבית השמאלית (הגבוהה מבחינת סדר הסיביות) מייצגת את הערך 128. ערכו הגבוה ביותר האפשרי של אוקטט הוא 255, וזה כאשר לכל הסיביות יש את הערך הבינרי 1, כפי שמתואר בתרשים 2.5.



תרשים 2.5 לכל הסיביות יש את הערך 1, מה שגורם לערך עשרוני כולל של 255

הטבלה הבאה מראה כיצד להמיר את הסיביות באוקטט אחד מקוד בינרי לערכים עשרוניים.

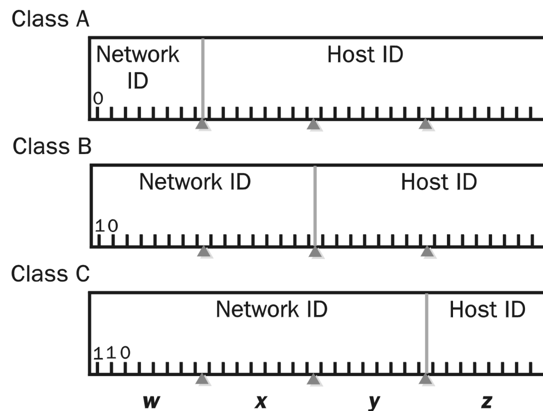
קוד בינרי	ערכי סיביות	ערך עשרוני
00000000	0	0
00000001	1	1
00000011	1+2	3
00000111	1+2+4	7
00001111	1+2+4+8	15
00011111	1+2+4+8+16	31
00111111	1+2+4+8+16+32	63
01111111	1+2+4+8+16+32+64	127
11111111	1+2+4+8+16+32+64+128	255

מחלקות כתובת

כתובות אינטרנט מוקצות על ידי גוף בשם InterNIC (www.internic.net), הארגון המנהל את רשת האינטרנט. כתובות IP אלו מחולקות למחלקות. המחלקות השכיחות ביותר הן A, B ו-C. מחלקות D ו-E קיימות, אך אינן בשימוש רגיל של משתמשי קצה. לכל אחת ממחלקות הכתובת יש כתובת Subnet Mask שונה. ניתן לזהות לאיזו מחלקה שייכת כתובת IP על ידי בחינת האוקטט הראשון שלה. לפניך רשימה של טווחי מחלקות A, B ו-C של כתובות האינטרנט, כאשר לכל אחת מהן מצורפת דוגמה לכתובת במחלקה זו:

- ❖ כתובות במחלקה A (Class A) משוייכות לרשתות גדולות מאוד, בהן מספר רב ביותר של מארחים. לרשתות Class A יש כברירת מחדל את Subnet Mask 255.0.0.0 והאוקטט הראשון בה יכול להיות 0-126. הכתובת 10.52.36.11 היא כתובת מ-Class A, מפני שהאוקטט הראשון שלה הוא 10, שהוא בין 0 ל- 126, כולל.
- ❖ כתובות במחלקה B (Class B) משוייכות לרשתות בינוניות בגודלן. לרשתות Class B יש כברירת מחדל את Subnet Mask 255.255.0.0 והאוקטט הראשון בה יכול להיות 128-191. הכתובת 172.16.52.63 היא כתובת מ- Class B, מפני שהאוקטט הראשון שלה הוא 172, שהוא בין 128 ל- 191, כולל.
- ❖ כתובות במחלקה C (Class C) משוייכות לרשתות LAN קטנות בגודלן. לרשתות Class C יש כברירת מחדל את Subnet Mask 255.255.255.0 והאוקטט הראשון בה יכול להיות 192-223. הכתובת 192.168.123.132 היא כתובת מ- Class C, מפני שהאוקטט הראשון שלה הוא 192, שהוא בין 192 ל- 223, כולל.

מחלקת הכתובת מגדירה אילו סיביות תשמשנה כמזהה רשת ואילו תשמשנה כמזהה מארח, כפי שמתואר בתרשים 2.6. המחלקה גם מגדירה את מספר הרשתות האפשריות, ואת מספר המארחים בכל רשת.



תרשים 2.6 כיצד מאורגנות הסיביות בכל מחלקת כתובות IP

ההבדלים בין כתובות המחלקות השונות מתוארים בתרשים 2.7.

	Number of Networks	Number of Hosts per Network	Range of Network IDs (First Octet)
Class A	126	16,777,214	1 – 126
Class B	16,384	65,534	128 – 191
Class C	2,097,152	254	192 – 223

תרשים 2.7 כיצד משפיעות מחלקות הכתובות על הרשת

קווים מנחים לכתובות IP

למרות שלא נחקקו חוקים לגבי אופן הקצאת כתובות IP, ודא כי הינך מקצה מזהה רשת ומזהה מארח תקפים. קיימים מספר קווים מנחים כלליים לפיהם עליך לפעול כאשר אתה מקצה מזהה רשת ומזהה מארח:

- מזהה הרשת אינו יכול להיות 127. מזהה זה שמור למטרות לולאה פנימית ופעילויות אבחון.
- לא ניתן שכל סיביות מזהה הרשת ומזהה המארח תקבענה לערך 1. אם לכל הסיביות נקבע הערך 1, מתורגמת הכתובת כ-Broadcast, ולא כמזהה מארח.
- לא ניתן שכל סיביות מזהה הרשת ומזהה המארח תקבענה לערך 0. אם לכל הסיביות נקבע הערך 0 מתורגמת הכתובת כ"רשת זו בלבד" (This network only).

- מזהה המארח חייב להיות ייחודי למזהה הרשת המקומי. נדרש מזהה רשת ייחודי לכל רשת וחיבור רחב. אם אתה מתחבר לרשת האינטרנט הציבורית, עליך לרכוש מזהה רשת מספק שירותי אינטרנט.
- כל מארחי TCP/IP, כולל ממשקים לנתבים, דורשים מזהה מארח ייחודי. מזהה המארח של הנתב הוא כתובת ה-IP המוגדרת כ- Default Gateway של תחנת העבודה.
- לכל מארח ברשת TCP/IP דרושה Subnet Mask, בין אם זו Subnet Mask המוגדרת כברירת מחדל, אשר בה נעשה שימוש כאשר הרשת אינה מחולקת לרשתות משנה, ובין אם זו Subnet Mask מותאמת אישית, ובה משתמשים כאשר מחלקים את הרשת ל-Subnets . Subnet Mask היא כתובת בת 32 סיביות המשמשת כדי לחסום, או "למסך", חלק מכתובת ה-IP, כדי להבדיל את מזהה הרשת ממזהה המארח. דבר זה נחוץ כדי ש-TCP/IP יוכל להבדיל אם כתובת IP כלשהי נמצאת ברשת המקומית או ברשת מרוחקת. ברירת המחדל של Subnet Mask בה תשתמש תלויה במחלקת הכתובת (Address Class), כפי שמתואר בתרשים 2.8.

Address Class	Bits Used for Subnet Mask				Dotted Decimal Notation
Class A	11111111	00000000	00000000	00000000	255.0.0.0
Class B	11111111	11111111	00000000	00000000	255.255.0.0
Class C	11111111	11111111	11111111	00000000	255.255.255.0

Class B Example

IP Address	131.107.	16.200
Subnet Mask	255.255.	0.0
Network ID	131.107.	y.z
Host ID	w.x.	16.200

תרשים 2.8 דוגמה ל- Subnet Mask המשמשת לכתובת IP מ- Class B

סיכום שיעור

כל מארח TCP/IP מזוהה על ידי כתובת IP לוגית, ונדרשת כתובת IP ייחודית עבור כל רכיב מארח המתקשר באמצעות TCP/IP. כל כתובת IP מגדירה את מזהה הרשת ומזהה המארח. כתובת IP היא באורך 32 סיביות וכולל שמונה מקטעים בני שמונה סיביות כל אחד, הנקראים אוקטט. קיימות חמש מחלקות כתובת. Microsoft תומכת בכתובות IP ממחלקות A, B ו-C המוקצות למארחים. כל מחלקת כתובת יכולה להכיל רשתות בגדלים שונים.

קיימים מספר קווים מנחים על פיהם עליך לפעול, כדי לוודא כי הינך מקצה כתובות IP חוקיות. לכל המארחים ברשת נתונה חייב להיות אותו מזהה רשת, כדי שיוכלו לתקשר בינם לבין עצמם. כל מארחי TCP/IP, כולל ממשקים לנתבים, חייבים מזהה מארח ייחודי.

שיעור 3: התקנה והגדרה של TCP/IP

שיעור זה יתאר את תהליך ההתקנה וההגדרה של Microsoft TCP/IP. עקוב אחר תהליך זה אם עדיין לא הזדמן לך לבצע התקנה של פרוטוקול התקשורת TCP/IP במחשב(ים) שלך בהם את משתמש לצורך תרגול ההליכים במהלך קורס זה.

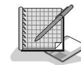
לאחר שיעור זה, תוכל

- להגדיר פרמטרים של TCP/IP.
- לזהות תוכניות שירות שכיחות של TCP/IP.
- לתאר את נושא סינון מנות.

זמן לימוד משוער: 15 דקות

התקנת TCP/IP

TCP/IP יכול לשמש בסביבת רשת LAN קטנה ועד לסביבת האינטרנט חובקת העולם. כאשר אתה מפעיל את תוכנית ההתקנה של Windows 2000, מותקן TCP/IP כפרוטוקול ברירת המחדל לרשת, אם במהלך ההתקנה זוהה כרטיס רשת. בשל כך, עליך לבצע התקנה של TCP/IP רק במקרה והבחירה האוטומטית בפרוטוקול זה בוטלה במהלך ההתקנה, או אם מחקת אותו (מסיבה זו או אחרת) מחיבור רשת מסוים בחלון Network and Dial-up Connections.



תרגול: התקנת פרוטוקול TCP/IP

בתרגול זה תתקין את פרוטוקול TCP/IP עבור Local Area Connection שבחלון Network and Dial-up Connections. כדי להשלים תרגול זה, עליך להיכנס למערכת כמנהל (Administrator) או כחבר בקבוצת המנהלים (Administrators Group).



לפני שתמשיך בשיעור, הפעל את קובץ ההדגמה Ch02.exe הנמצא בתיקיה Media שבתקליטור המצורף לספר זה. הקובץ יספק סקירה אודות התקנת פרוטוקול TCP/IP.

טיפ להפעלת הקובץ, צריך שבמחשב שלך יהיה מותקן כונן תקליטורים אליו מחוברות אוזניות, או שהוא מחובר לכרטיס קול אליו מחוברים רמקולים.

➤ **להתקנת TCP/IP עבור חיבור הרשת המקומי שלך**

1. לחץ על Start, הצבע על Settings, ובחר Network and Dial-up Connections.

   תיבת הדו-שיח Network and Dial-up Connections מופיעה.

2. לחץ לחיצה ימנית על Local Area Connection, ומתפריט הקיצור בחר Properties.

   תיבת הדו-שיח Local Area Connection Properties מופיעה.

3. לחץ על Install. תיבת הדו-שיח Select Network Component Type מופיעה.

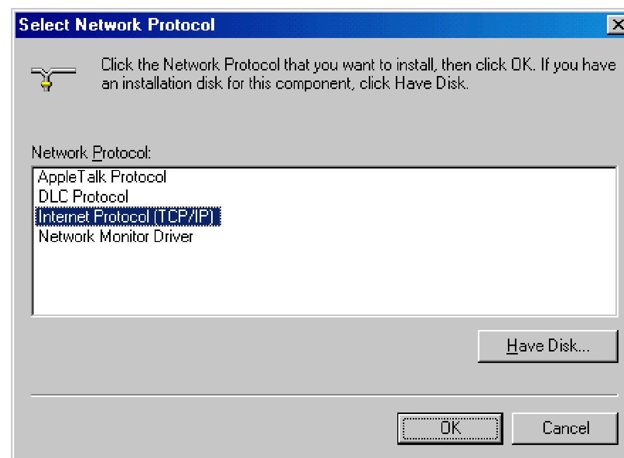
4. לחץ על Protocol, ולחץ על Add.

תיבת הדו-שיח Select Network Protocol מופיעה.

5. לחץ על Internet Protocol (TCP/IP), כפי שמוצג בתרשים 2.9, ולחץ על OK.

פרוטוקול TCP/IP מותקן ונוסף לרשימה Components שבתיבת הדו-שיח Local Area Connection Properties.

6. לחץ על Close.



תרשים 2.9 בחירת Internet Protocol (TCP/IP)

הגדרת TCP/IP

אם אתה מיישם את TCP/IP בפעם הראשונה ברשת שלך, עליך ליצור תוכנית פעולה מפורטת עבור מיעון IP (IP Addressing) של הרשת. סכמת המיעון של רשת TCP/IP שלך יכולה לכלול כתובות IP ציבוריות או פרטיות. אתה יכול לבחור להשתמש בכתובות פרטיות או ציבוריות, אם הרשת שלך אינה מיועדת להיות מחוברת לאינטרנט. אבל, רוב הסיכויים שתגדיר מספר כתובות ציבוריות לשם תמיכה בהתחברות לאינטרנט. תעשה זאת מפני שהתקנים המחוברים ישירות לאינטרנט דורשים כתובת IP ציבורית. ארגון InterNIC מקצה כתובות ציבוריות לספקי שירותי אינטרנט (ISP). אלו, מצידם, מקצים כתובות IP לארגונים, כאשר אותם ארגונים רוכשים התחברות לאינטרנט. ייחודיות כתובות IP המוקצות בדרך זו מובטחת, והן מתוכנתות לנתבי אינטרנט כדי שתעבורת הרשת תועבר ישירות למארח היעד המתאים.

מעבר לכך, תוכל ליישם סכמת מיעון פרטית, כדי להגן על הכתובות הפנימיות שלך מיתר הגולשים באינטרנט, וזאת על ידי הקצאת כתובות פרטיות בכל הרשת הפרטית שלך (או האינטראנט). כתובות פרטיות אינן נגישות למשתמשים באינטרנט, מפני שהן נפרדות מהכתובות הציבוריות, ואינן חופפות להן.

תוכל להקצות כתובות IP בסביבת Windows 2000 באופן דינמי, תוך שימוש ב- DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol), ותוכל למען הקצאות באמצעות APIPA (**A**utomatic **P**rivate **IP** **A**ddressing). תוכל גם להגדיר את TCP/IP באופן ידני. אתה מגדיר את TCP/IP במחשב, בהתאם לתפקידו של המחשב. למשל, מתרים ביחסי שרת/לקוח בארגון צריכים שתוקצה להם כתובת IP באופן ידני. אבל, תוכל להגדיר את TCP/IP באופן דינמי באמצעות שרת DHCP עבור רוב הלקוחות ברשת.

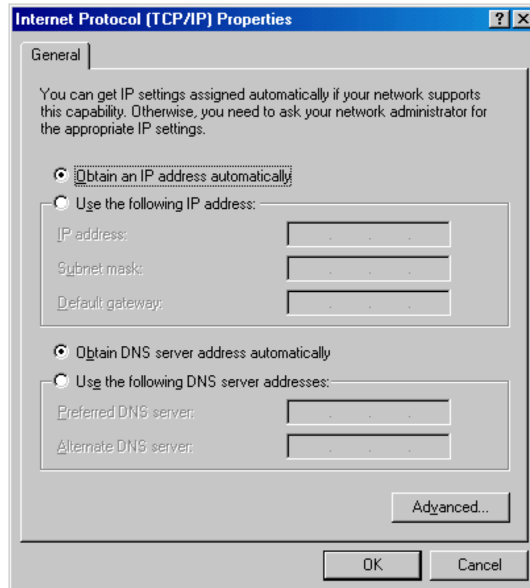
הגדרה דינמית

כברירת מחדל, מחשבים הפועלים בסביבת Windows 2000 ינסו לקבל הגדרת TCP/IP משרת DHCP ברשת, כפי שמתואר בתרשים 2.10. אם כרגע מיושמת הגדרת TCP/IP ידנית במחשב, תוכל ליישם בו הגדרה דינמית.

➢ ליישום הגדרה דינמית של TCP/IP

1. לחץ על Start, הצבע על Settings, ולחץ על Network and Dial-up Connections.
2. לחץ לחיצה ימנית על Local Area Connection, ומתפריט הקיצור בחר Properties.
3. בכרטיסיה General, לחץ על Internet Protocol (TCP/IP), ולחץ על Properties.

   עבור חיבורים מסוג אחר, בחר בכרטיסיה Networking.
4. לחץ על Obtain an IP address automatically, ולחץ OK.



תרשים 2.10 הגדרת המחשב שלך, כך שיקבל הגדרות TCP/IP באופן אוטומטי

הגדרה ידנית

לשרתים מסוימים, כגון DHCP, DNS או WINS, יש להקצות כתובת IP באופן ידני וקבוע. אם אין לך שרת DHCP ברשת, עליך להגדיר את TCP/IP במחשבים באופן ידני, כך שישתמשו בכתובת IP קבועה.

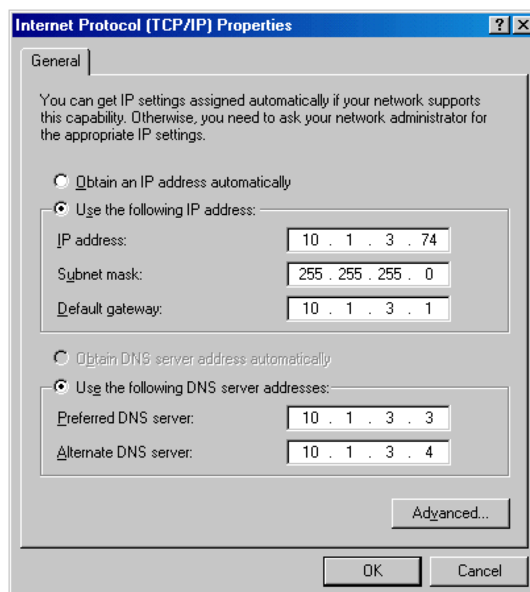
להגדרת מחשב TCP/IP לשימוש בכתובת IP קבועה

1. לחץ על Start, הצבע על Settings, ולחץ על Network and Dial-up Connections.
2. לחץ לחיצה ימנית על Local Area Connection, ומתפריט הקיצור בחר Properties.
3. בכרטיסיה General לחץ על Internet Protocol (TCP/IP), ולחץ על Properties.
4. לחץ על Use the following IP address.

כעת יהיה עליך להקליד כתובת IP, Subnet Mask ו- Default Gateway. אם ברשת שלך פועל שרת DNS, תוכל להגדיר את המחשבים שלך להשתמש ב-DNS.

להגדרת המחשב לשימוש ב-DNS

1. לחץ על Use the following DNS server addresses.
2. בתיבות Preferred DNS server ו- Alternate DNS server, הקלד את כתובות שרת DNS ראשי (Primary) ומשני (Secondary), כפי שמתואר בתרשים 2.11.



תרשים 2.11 הגדרה ידנית של TCP/IP במחשב שלך

תוכל גם להגדיר כתובות IP ו- Default Gateways נוספים, על ידי ביצוע ההליך הבא.

➤ **להגדרת כתובות IP ו- Default Gateways נוספים**

1. בתיבת הדו-שיח Internet Protocol (TCP/IP) Properties לחץ על Advanced.
2. בכרטיסיה IP Settings בתיבה IP Addresses לחץ על Add.
3. בתיבות IP Address ו- Subnet Mask הקלד כתובת IP וכתובת Subnet Mask, ולחץ על Add.
4. חזור על צעדים 2 ו-3 עבור כל כתובת IP שברצונך להוסיף. לסיום לחץ על OK.
5. בכרטיסיה IP Settings בתיבה Default Gateways, לחץ על Add.
6. בתיבות Gateway ו- Metric הקלד כתובת IP של Default Gateways ומאפייניו (Metric), ולחץ על Add.

   עליך להקליד ערך מאפיין Metric גם בתיבה Interface Metric, כדי להגדיר מטריקה מותאמת עבור התחברות זו.
7. חזור על צעדים 5 ו-6 עבור כל כתובת IP שברצונך להוסיף. לסיום לחץ על OK.

הערה בפרק 9 תלמד בהרחבה כיצד להגדיר לקוח להשתמש בשרת WINS.

Automatic Private IP Addressing

אפשרות נוספת למיעון TCP/IP היא השימוש ב-APIPA (**A**utomatic **P**rivate **IP A**ddressing), כאשר DHCP אינו זמין. בגרסאות קודמות של Windows, הגדרת כתובת IP יכולה היתה להתבצע באופן ידני או באופן דינמי באמצעות DHCP. אם לא היתה ללקוח אפשרות לקבל כתובת IP באופן דינמי משרת DHCP, שירותי הרשת עבור אותו לקוח היו לא זמינים. התכונה APIPA של Windows 2000 ממכנת את תהליך הקצאת כתובת IP שאינה בשימוש, למקרה בו שרת DHCP אינו זמין.

כתובת APIPA נבחרת מתוך בלוק הכתובות השמורות 169.254.0.0 של Microsoft, עם Subnet Mask 255.255.0.0. כאשר נעשה שימוש בתכונה APIPA של Windows 2000 מוקצת ללקוח כתובת בטווח שבין 169.254.0.1 ועד 169.254.255.254. כתובת IP המוקצת משמשת את הלקוח עד אשר מאותר שרת DHCP. בכל מקרה, ה- Subnet Mask של ברירת המחדל היא 255.255.0.0, באופן אוטומטי.

תהליך זה מאפשר ללקוח להמשיך ולתפקד גם במצב בו שרת DHCP אינו זמין. ברגע שהלקוח מזהה ששרת DHCP אינו זמין הוא יוצר לעצמו כתובת IP ומוודא שאין כתובת כזו ברשת (כדי למנוע התנגשויות). במידה ונמצא שכתובת כזו קיימת, יוצר הלקוח לעצמו כתובת IP חדשה ותהליך הבדיקה מתחיל מחדש.

בדיקת TCP/IP באמצעות Ipconfig ו-PING

כדי להבטיח שהמחשבים שלך יכולים לתקשר עם מארחי TCP/IP אחרים ברשת, עליך לבצע בדיקה של הגדרות TCP/IP שלך. תוכל לבצע בדיקת הגדרה בסיסית באמצעות תוכניות השירות Ipconfig ו-PING.

תוכנית השירות IPCONFIG מוודאת את תקינותן של הגדרות הפרמטרים של TCP/IP, כולל כתובת IP, Subnet Mask ו- Default Gateway, ממנחה שורת הפקודה (Command Prompt). פעולה זו יעילה כדי לקבוע אם ההגדרות אותחלו כהלכה, או אם הוגדרה בטעות כפילות של כתובת IP.

➢ שימוש ב-Ipconfig משורת הפקודה

1. פתח חלון Command Prompt.
2. במנחה שורת הפקודה הקלד ipconfig, והקש Enter. נתוני הגדרות TCP/IP מוצגים במסך, כפי שניתן לראות בתרשים 2.12.

```
C:\WINNT.0\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.1.3.74
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.1.3.1

C:\>_
```

תרשים 2.12 שימוש ב-Ipconfig להצגת נתוני תצורת TCP/IP

במידה וכתובה לשלב 2 הקודם מוצג הערך 0.0.0.0 עבור Subnet Massk, יש להבין מכך שלמחשב כלשהו ברשת מוגדרת כתובת IP זהה לזו המוגדרת במחשב בו הפעלנו את Ipconfig.

לאחר שתוודא את הגדרות TCP/IP באמצעות תוכנית השירות Ipconfig, תוכל להשתמש בתוכנית השירות PING כדי לבחון את החיבוריות. תוכנית השירות PING היא כלי אבחון הבוחן את הגדרות TCP/IP ומאבחן כשלים בחיבוריות. PING משתמשת בהודעות Echo Request ו- Echo Reply של ICMP (**I**nternet **C**ontrol **M**essage **P**rotocol) כדי לקבוע אם מארח TCP/IP מסוים זמין ומתפקד. כמו תוכנית השירות IPCONFIG, גם PING מופעלת ממנחה שורת הפקודה. תחביר הפקודה הוא:

ping IP_Address

אם בדיקת PING עוברת בהצלחה, תופיעה במסך הודעה דומה לזו שבתרשים 2.13.

```
C:\WINNT.0\System32\cmd.exe
Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.1.3.74
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.1.3.1

C:\>ping 10.1.3.1

Pinging 10.1.3.1 98.2 with 32 bytes of data:

Reply from 10.1.3.1: bytes=32 time<10ms TTL=128
Reply from 10.1.3.1: bytes=32 time<10ms TTL=128
Reply from 10.1.3.1: bytes=32 time<10ms TTL=128
Reply from 10.1.3.1: bytes=32 time<10ms TTL=128

Ping statistics for 10.1.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
C:\>_
```

תרשים 2.13 הודעות תגובה המוצגות על ידי תוכנית השירות PING

כדי לזהות תקלות נשתמש, קודם כל, בפקודה Ipconfig (כדי לזהות את כתובת ה-IP של המחשב בו אנו עובדים) ולאחר מכן נבדוק את תקינות פעולת הרשת באמצעות הפקודה PING.

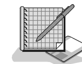
הגדרת מסנני מנות

ניתן להשתמש בסינון מנות IP כדי להפעיל מו״מ אבטחה (Security Negotiation) עבור תקשורת מבוססת מקור, יעד וסוג תעבורת IP. דבר זה מאפשר לקבוע איזו הפעלת תעבורת IP או IPX תהיה מאובטחת, חסומה או שיורשה לה לעבור ללא סינון.

לדוגמה, תוכל להגביל את סוג הגישה אל ומאת הרשת לתעבורה מוגבלת למערכות נבחרות. עליך לוודא שאינך מגדיר מסנני מנות מגבילים מדי, אשר עלולים לפגוע בפעילותם של פרוטוקולים חשובים במחשב. למשל, אם מחשב הפועל בסביבת Windows 2000 גם מפעיל את IIS (**I**nternet **I**nformation **S**ervices) כשרת אינטרנט, ומסנן המנות מוגדר כך שרק תעבורה מבוססת אינטרנט מורשית לעבור, לא תוכל להשתמש ב-PING (אשר עושה שימוש ב- Echo Request ו- Echo Reply של ICMP) כדי לבצע אבחון תקלות בסיסי.

תוכל להגדיר את פרוטוקול TCP/IP לסינון מנות IP על פי:

- מספר יציאת TCP (TCP Port)
- מספר יציאת UDP (UDP Port)
- מספר פרוטוקול IP



תרגול: יישום מסנני מנות IP

בתרגול זה תיישם סינון מנות TCP/IP במחשב Windows 2000 Server עבור חיבור LAN.

➢ ליישום סינון מנות TCP/IP

1. לחץ על Start, הצבע על Settings, ולחץ על Network and Dial-Up Connections.
2. לחץ לחיצה ימנית על Local Area Connection, ומתפריט הקיצור בחר Properties.

   תיבת דו-שיח Local Area Connection Properties מופיעה.
3. סמן את Internet Protocol (TCP/IP), ולחץ על Properties.

   תיבת דו-שיח Internet Protocol (TCP/IP) Properties מופיעה.
4. לחץ על Advanced.

   תיבת דו-שיח Advanced TCP/IP Settings מופיעה.
5. בחר בכרטיסיה Options, בחר TCP/IP Filtering, ולחץ על Properties.

   תיבת דו-שיח TCP/IP Filtering מופיעה, כפי שנראה בתרשים 2.14.

6. לחץ על Enable TCP/IP Filtering (All Adapters).

כעת תוכל להוסיף סינון TCP, UDP או פרוטוקול IP על ידי לחיצה על אפשרות Permit Only ואז לחיצה על Add מתחת לרשימות TCP, UDP או IP Protocols.

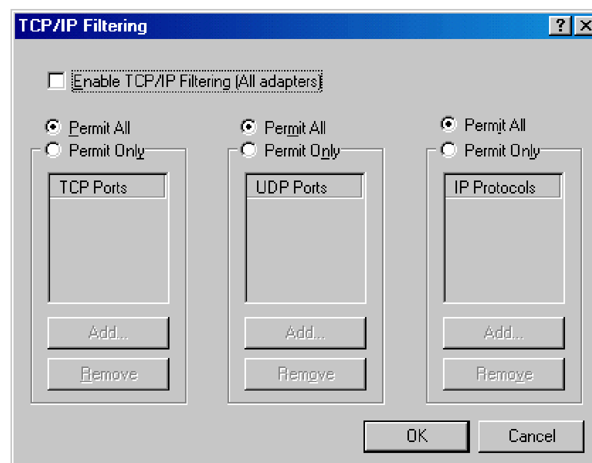
חלק מיישומי סינון TCP/IP אותם תוכל ליישם כוללים:

- אפשור (Enabling) TCP רק ביציאה 23 (Port 23), מה שיסנן את כל התעבורה, חוץ מתעבורת Telnet.
- אפשור TCP רק ביציאה 80 בשרת אינטרנט ייעודי, כדי שיעבד תעבורת TCP מבוססת אינטרנט בלבד.

אזהרה אם תאפשר רק את יציאה 80 (Port 80) של TCP/IP, תהיה כל תקשורת הרשת שאינה עוברת ביציאה 80 לא זמינה.

---

7. לחץ OK בכל תיבות הדו-שיח כדי לסגור אותן.



תרשים 2.14 הגדרת סינון מנות TCP/IP בתיבת הדו-שיח TCP/IP Filtering

סיכום שיעור

כברירת מחדל, מותקן פרוטוקול TCP/IP בעת התקנת מערכת ההפעלה Windows 2000, במידה ומאותר כרטיס רשת. ניתן להתקין את פרוטוקול TCP/IP גם באופן ידני. לאחר התקנת TCP/IP במחשב תוכל להגדיר אותו, כך שיקבל כתובת IP באופן אוטומטי או שתגדיר את תצורת הפרוטוקול באופן ידני. בנוסף, תוכל גם ליישם סינון מנות כדי להגביל את סוג הגישה אל ומאת הרשת, וזאת כדי להגביל גישה למערכות מסוימות.

שיעור 4: עקרונות בסיסיים בניתוב IP

ניתוב (Routing) הוא תהליך של בחירת הנתיב דרכו יועברו מנות הנתונים, וזו פעילותו העיקרית של פרוטוקול האינטרנט, IP. הנתב (Router), שלעיתים מתייחסים אליו כאל שער, (Gateway) הוא התקן המעביר (Forward) את המנות מרשת פיסית אחת לאחרת. כאשר נתב מקבל מנה, מעביר מתאם (כרטיס) הרשת את צרור הנתונים (Datagram) לשכבת IP. IP בוחן את כתובת היעד שבצרור הנתונים ומשווה אותה עם טבלת ניתוב ה-IP שלו. אז מתבצעת החלטה לגבי היעד אליו יש להעביר את המנה. שיעור זה יסביר לך עקרונות בסיסיים בניתוב IP.

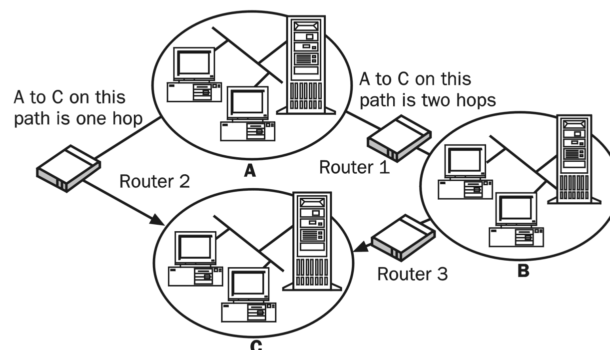
לאחר שיעור זה, תוכל

- לעדכן טבלת ניתוב מבוסס Windows 2000 באמצעות נתיבים קבועים.
- לנהל ולנטר ניתוב פנימי.
- לנהל ולנטר ניתוב גבולי.

זמן לימוד משוער: 40 דקות

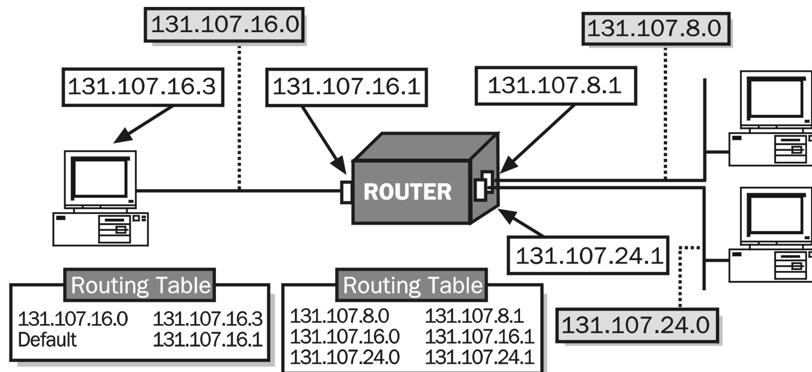
סקירת נושא הניתוב

הנתב (Router) מסייע לרשתות LAN או WAN להשיג את יכולת העבודה עם סביבות שונות ואת החיבוריות, והוא יכול לקשר בין רשתות מקומיות (LAN) בעלות טופולוגיות שונות, כגון Ethernet ו- Token Ring. לכל מנה הנשלחת ב-LAN יש כותרת (Packet Header) המכילה שדה כתובת מקור ושדה כתובת יעד. הנתב מתאים בין כותרות המנה למקטע LAN (LAN Segment) ובוחר את הנתיב הטוב ביותר עבור המנה, וכך משפר את ביצועי הרשת. למשל, אם מנה נשלחת ממחשב A למחשב C, כפי שניתן לראות בתרשים 2.15, יהיה בנתיב הטוב ביותר דילוג (Hop) אחד בלבד. אם נתב 1 הוא נתב ברירת המחדל עבור מחשב A, תנותב המנה דרך נתב 2. מחשב A יקבל הודעה לגבי הנתיב הטוב יותר דרכו עליו לשלוח את המנות למחשב C. בכל פעם שמאותר נתיב, נשלחת המנה לנתב הבא (הדבר נקרא Hop, או דילוג בעברית), עד אשר היא מגיעה בסופו של דבר למארח היעד. אם לא אותר נתיב, נשלחת הודעת שגיאה למארח המקור.



תרשים 2.15 מנה מנותבת ממחשב A למחשב C

כדי לקבל החלטות ניתוב, מתייעצת שכבת ה-IP עם טבלת ניתוב המאוחסנת בזיכרון, כפי שניתן לראות בתרשים 2.16.



תרשים 2.16 שכבת IP מתייעצת עם טבלת הניתוב

טבלת הניתוב מכילה רשומות עם כתובות ה-IP של ממשקי ניתוב ברשתות אחרות איתן היא יכולה לתקשר. טבלת ניתוב היא סדרת רשומות, הנקראות נתיבים (Routes), המכילות את המידע אודות מיקומם של מזהי הרשת (Network ID) ברחבי הרשת. טבלת הניתוב במחשב הפועל בסביבת Windows 2000 נבנית באופן אוטומטי, בהתאם להגדרת TCP/IP של אותו מחשב. ניתן לצפות בתוכן טבלת הניתוב, על ידי הקלדת הפקודה router print במנחה שורת הפקודה, כפי שניתן לראות בתרשים 2.17.

```
C:\WINNT.0\System32\cmd.exe
(C) Copyright 1985-1999 Microsoft Corp.

C:\>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x1000003 ...00 50 04 94 ec 1d ...... FE575 Ethernet Adapter
0x2000004 ...00 53 45 00 00 00 ...... WAN (PPP/SLIP) Interface
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    10.33.238.171   10.33.238.171       1
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
     10.33.224.19  255.255.255.255    10.33.238.171   10.33.238.171       1
    10.33.238.171  255.255.255.255        127.0.0.1       127.0.0.1       1
    10.33.255.255  255.255.255.255    10.33.238.171   10.33.238.171       1
        224.0.0.0        224.0.0.0    10.33.238.171   10.33.238.171       1
  255.255.255.255  255.255.255.255    10.33.238.171         1000003       1
Default Gateway:     10.33.238.171
===========================================================================
Persistent Routes:
  None

C:\>_
```

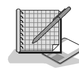
תרשים 2.17 הצגת טבלת הניתוב ממנחה שורת הפקודה

הערה טבלת הניתוב אינה ייחודית לנתב. גם למארחים יש טבלת ניתוב המשמשת לקביעת הנתיב האופטימלי

ניתוב דינמי וניתוב קבוע

התהליך בו נעזרים הנתבים לאיתור נתוני הניתוב הוא שונה, בהתבסס על השאלה אם הנתב מבצע ניתוב IP קבוע, או ניתוב IP דינמי. ניתוב קבוע (Static Routing) הוא פעולה של IP, אשר מגבילה אותך לטבלת נתיבים קבועים. ניתוב קבוע דורש שטבלאות הניתוב ייבנו ויעודכנו באופן ידני. כדי להוסיף נתיבים קבועים לטבלת ניתוב, עליך להשתמש בפקודה ROUTE, המופעלת ממנחה שורת הפקודה.

כדי להוסיף או לשנות נתיב קבוע	פעולה
route add [network] mask [netmask][gateway]	מוסיף נתיב
route -p add [network] mask [netmask][gateway]	מוסיף נתיב מתמיד (Persistant Route)
route delete [network] [gateway]	מוחק נתיב
route change [network] [gateway]	משנה נתיב
route print	מציג את טבלת הניתוב
route -f	מוחק את כל הנתיבים מהטבלה



תרגול: עדכון טבלת ניתוב במחשב מבוסס Windows 2000

בתרגול זה תעדכן טבלת ניתוב במחשב מבוסס Windows 2000 באמצעות נתיבים קבועים.

לעדכון טבלת ניתוב

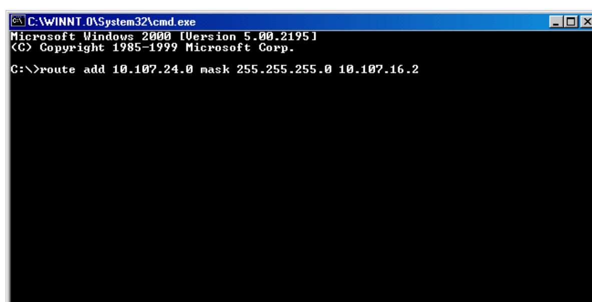
1. פתח חלון שורת פקודה (Command Prompt).
2. במנחה שורת הפקודה הקלד את הפקודה:

route add *IP_Address* mask *Subnet_Mask GateWay*

כדי להוסיף נתיב לשם אפשור ההתקשרות עם רשת ממארח ברשת אחרת.
לדוגמה, כדי להוסיף נתיב לאפשור ההתקשרות מארח ברשת 10.107.16.0 עם רשת 10.107.24.0 יהיה עליך להקליד את הפקודה:

route add 10.107.24.0 mask 255.255.255.0 10.107.16.2

כפי שנראה בתרשים 2.18.



תרשים 2.18
הוספת נתיב קבוע
לטבלת הניתוב

שימוש בניתוב דינמי

אם נתיב משתנה, נתבים קבועים אינם מידעים אחד את השני לגבי השינוי. מעבר לכך, נתבים קבועים אינם מחליפים נתיבים עם נתבים דינמיים. להיפך, ניתוב דינמי מעדכן באופן דינמי את טבלאות הניתוב, ובכך מפחית את תדירות הניהול. אבל, ניתוב דינמי מגביר את העומס על הרשת ברשתות גדולות.

פרוטוקולי ניתוב

ניתוב דינמי הוא פעילות של פרוטוקולי ניתוב, כגון RIP (**R**outing **I**nformation **P**rotocol) ו- OSPF (**O**pen **S**hortest **P**ath **F**irst). מדי פעם מחליפים פרוטוקולי הניתוב נתיבים לרשתות ידועות בין נתבים דינמיים. אם נתיב כלשהו משתנה, הנתבים האחרים מיודעים אודות השינוי באופן אוטומטי. במחשבים מבוססי Windows 2000 Server או Windows 2000 Advanced Server המשמשים כנתבים חייבים להיות מותקנים מספר מתאמי רשת (אחד לכל רשת). בנוסף, עליך להתקין ולהגדיר את השירות Routing and Remote Access, מפני שפרוטוקולי הניתוב אינם מותקנים באופן אוטומטי בעת התקנת Windows 2000. תלמד כיצד לישם ניתוב IP למשתמשים מרוחקים בפרק 11.

Windows 2000 מאפשרת לך לבחור בין שני פרוטוקולי ניתוב IP עיקריים, בהתאם לגודל הרשת או הטופולוגיה בה היא בנויה. שני הסעיפים הבאים יסבירו את פרוטוקולי הניתוב הללו.

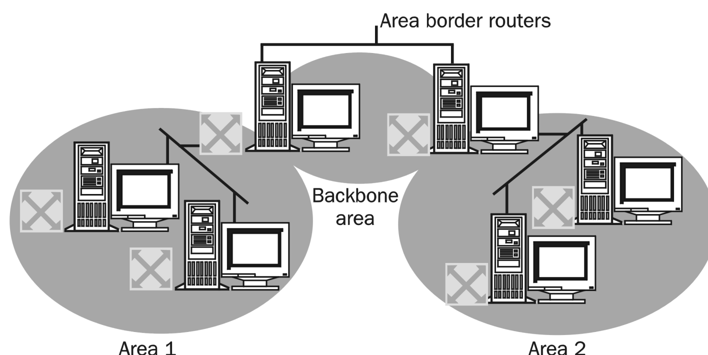
(RIP) Routing Information Protocol

RIP הוא פרוטוקול ניתוב תלוי-מרחק (Distance-Vector Routing Protocol) המסופק מטעמי תאימות לאחור עם רשתות RIP קיימות. RIP מאפשר לנתב להחליף נתוני ניתוב עם נתבי RIP אחרים, כדי לגרום להם להיות ערים לשינויים במבנה הכולל של הרשת. RIP משדר (Broadcast) את המידע לנתבים שכנים, ומדי פרק זמן קצוב שולח מנות שידור RIP המכילות את כל נתוני הניתוב הידועים לנתב. שידורים אלה שומרים על הסינכרון בין כל הנתבים ברשת הגדולה.

(OSPF) Open Shortest Path First

OSPF הוא פרוטוקול ניתוב מצב-קישור (Link-State Routing Protocol) המאפשר לנתבים להחליף ביניהם נתוני ניתוב, וליצור מפה של הרשת המחשבת את הנתיב האפשרי הטוב ביותר לכל רשת. מייד בעת קבלת השינויים למסד נתוני מצב הקישור מחושבת מחדש טבלת הניתוב. ככל שגדל גודלו של מסד נתוני מצב הקישור, כך גם גדלות הדרישות לזיכרון ולזמני עיבוד הנתיבים. כדי לענות על בעיית גדילה זו, מחלק OSPF את הרשת הגדולה לאוסף של רשתות רציפות, הנקראות אזורים (Areas). אזורים מחוברים בינם לבין עצמם באמצעות אזור רשת התשתית (Backbone Area). נתבי רשת התשתית (Backbone Routers) כוללים נתבים המחוברים ליותר מאשר אזור אחד. אבל, נתבי רשת התשתית אינם חייבים להיות נתבי גבול אזור (Area Border Routers). נתבים בהם כל הרשתות מחוברות לרשת התשתית הם נתבים פנימיים.

כל נתב שומר מסד נתוני מצב קישור רק עבור אותם אזורים המחוברים לנתב. נתבי גבול אזור (**A**rea **B**order **R**outers ,ABR) מחברים את אזור רשת התשתית לאזורים אחרים, כפי שניתן ללמוד מתרשים 2.19.



תרשים 2.19 תרשים בסיסי של אזור OSPF

סביבה מנותבת-OSPF היא הטובה ביותר עבור רשתות גדולות עד גדולות מאוד, מרובות נתיבים בהן IP דינמיים, כגון רשת ארגונית רחבה, קמפוס לימודים גדול, ארגון לו סניפים המפוזרים ברחבי העולם וכדומה. כדי לנהל את הנתבים הפנימיים (Internal Routers) ואת נתבי הגבול (Border Routers):

- ❖ ודא שה-ABR של האזור מוגדרים עם ההגדרות המתאימות (יעד, Subnet Mask) אשר מסכמים את נתיבי האזור.
- ❖ ודא שמסנני המקור והניתוב המוגדרים ב-ABR אינם מחמירים יתר על המידה, ובכך מונעים מנתיבים יעילים להיות מופצים למערכת האוטונומית של OSPF. סינון ניתוב ומקורות חיצוניים מוגדר בכרטיסיה External Routing שבתיבת הדו-שיח OSPF Routing Protocol Properties.
- ❖ ודא כי כל ה-ABR מחוברים לרשת התשתית (Backbone) פיסית או לוגית (באמצעות קישור וירטואלי). אלה לא צריכים להיות נתבי דלת-אחורית (Backdoor Routers), שהם נתבים המחברים שני אזורים מבלי שיעברו דרך רשת התשתית.

➤ כדי לנהל נתב

1. לחץ על Start, הצבע על Programs, הצבע על Administrative Tools, ולחץ על Routing and Remote Access.
2. ב- MMC Tree לחץ לחיצה ימנית על Server Status, ומתפריט הקיצור בחר Add Server.
3. בתיבת הדו-שיח Add Server פעל באחת מהדרכים הבאות:

- לחץ על The following computer, ואז הקלד את שם המחשב או את כתובת ה-IP של השרת.
- לחץ על All routing and remote acceess servers in the domain, ואז הקלד את שם ה- Domain המכיל את השרת אותו אתה מעוניין לנהל. לחץ OK, ובחר בשרת.

- לחץ על Browse the active directory, לחץ Next, ובתיבת הדו-שיח Find routers or remote access servers סמן את תיבות הסימון שליד סוגי השרתים אחריהם אתה מעוניין לחפש. לחץ OK ובחר בשרת.

4. תוכל לנהל שרת מרוחק מרגע שהוא מופיע כפריט ב- MMC Tree.

סיכום שיעור

נתבים (Routers) מעבירים מנות מרשת פיסית אחת לאחרת. שכבת IP מתייעצת עם טבלת ניתוב (Routing Table) המאוחסנת בזיכרון. טבלת ניתוב מכילה רשומות ובהן כתובות IP של ממשקי ניתוב לרשתות אחרות. נתבים קבועים (Static Routers) דורשים שטבלאות הניתוב ייבנו ויעודכנו באופן ידני. במקרה של ניתוב דינמי, אם נתיב משתנה, מיודעים הנתבים האחרים אודות השינוי באופן אוטומטי.

שאלות סיכום

השאלות הבאות נועדו לחזק את הנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות על שאלה, עיין בשיעור המתאים ונסה את השאלה שנית. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואחר כך בעברית.

Answering the following questions will reinforce key information presented in this chapter. If you are unable to answer a question, review the appropriate lesson and then try the question again. Answers to the questions can be found in Appendix A, "Questions and Answers".

1. What is TCP/IP?
2. Which TCP/IP utilities are used to verify and test a TCP/IP configuration?
3. What is the purpose of a subnet mask?
4. What is the minimum number of areas in an OSPF internetwork?
5. What is an internal router?
6. What is a border router?
7. What Windows 2000 administrative tool can you use to manage internal and border routers?

1. מהו TCP/IP?
2. איזה תוכניות שירות של TCP/IP משמשות כדי לבדוק ולוודא הגדרות TCP/IP?
3. מהי מטרת Subnet Mask?
4. מהו מספר האזורים המינימלי של אזורים ברשת OSPF?
5. מהו נתב פנימי?
6. מהו נתב גבולי?
7. איזה כלי ניהול של Windows 2000 יכול לשמש לניהול נתבים פנימיים ונתבי גבול?

פרק 3

יישום NWLink

אודות פרק זה

פרק זה יסקור את העבודה בסביבה מעורבת של Windows 2000 של Microsoft עם NetWare של Novell. כחלק מפרק זה תלמד כיצד להתקין ולהגדיר את פרוטוקול NWLink.

לפני שתתחיל

להשלמת פרק זה עליך:

- להשלים את תהליכי ההתקנה שבחלק **אודות ספר זה**.

שיעור 1: סקירת NWLink

אם חלק ממשאבי הרשת שלך נמצאים ברשת NetWare, תצטרך הרשת מבוססת Windows 2000 שלך לתקשר ולשתף משאבים עם רשת NetWare. Novell משתמשת בפרוטוקול IPX/SPX (**I**nternetwork **P**acket E**x**change/**S**equenced **P**acket E**x**change) כפרוטוקול הרשת העיקרי שלה. NWLink הוא פרוטוקול תואם-IPX/SPX שפותח על ידי Microsoft כדי לאפשר למחשבים מבוססי Windows 2000 לתקשר עם שירותי NetWare. שיעור זה סוקר את פרוטוקול NWLink.

לאחר שיעור זה, תוכל

- להסביר את מטרתו של פרוטוקול NWLink.
- לציין חלק מהמרכיבים המשמשים לשיתוף פעולה בין מחשבים מבוססי Windows 2000 לבין רשתות NetWare של Novell.
- לזהות את ארכיטקטורת NWLink.

זמן לימוד משוער: 25 דקות

יכולת הפעולה ההדדית עם NetWare

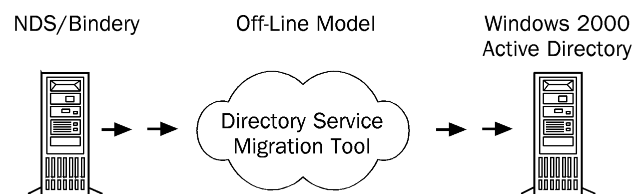
Windows 2000 מספקת פרוטוקולים ושירותים המאפשרים לך לשלב רשתות מבוססות Windows 2000 עם רשתות NetWare של Novell. היא מציגה את NWLink (פרוטוקול תעבורה תואם IPX/SPX/NetBIOS), את Gateway Service for NetWare ואת Client Service for NetWare של Windows 2000. תכונות אלו מאפשרות לך ליצור סביבת רשת משולבת, המורכבת משרתים מבוססי Windows 2000 ומשרתים מבוססי NetWare. תוכל גם להגר חשבונות משתמשים, קבוצות, קבצים והרשאות מ-NetWare ל- Windows 2000, תוך שימוש ב- Directory Services Migration Tool for NetWare המסופק עם Windows 2000.

הרשימה הבאה מתארת שירותים עבור Windows 2000 Server המאפשרים למחשבים הפועלים בסביבת Windows 2000 להתקיים ולתקשר עם רשתות ושרתי NetWare של Novell. כמה מהשירותים המתוארים ברשימה מהווים חלק ממערכת ההפעלה Windows 2000 Server, ואת האחרים ניתן למצוא כמוצרים נפרדים.

- **NWLink** (IPX/SPX/NetBIOS Compatible Transport Protocol). NWLink, פרוטוקול תואם-IPX/SPX, הוא אבן היסוד לשירותים תואמי NetWare בפלטפורמת Windows 2000. NWLink מהווה חלק בלתי נפרד מכל אחת ממהדורות Windows 2000 ומאפשר גישה ליישומים בשרתי Novell.
- **Gateway Service for NetWare.** גם שירות זה מהווה חלק בלתי נפרד מכל אחת ממהדורות Windows 2000. הוא מאפשר למחשב הפועל בסביבת Windows 2000 Server לתקשר ברמת שכבת היישום (Application Layer) עם שרתים הפועלים בסביבת NetWare 3.2 או גירסה מאוחרת יותר. נכללת גם תמיכה בתסריטי כניסה למערכת (Logon Script Support). בנוסף, ניתן להשתמש בשירות זה כדי ליצור Gateways

למשאבי NetWare, מה שיאפשר למחשבים בהם פועלים רק שירותי הלקוח של Microsoft לקבל גישה למשאבי ויישומי NetWare באמצעות ה- Gateway. Gateway Service for NetWare נדון ביתר פירוט בשיעור 2.

- **Directory Service Migration Tool.** כלי שירות זה מאפשר לך להגר (Migrate) חשבונות משתמשים, קבוצות, קבצים והרשאות משרת NetWare ל- Active Directory של Windows 2000. Windows 2000 מחליפה את הכלי NetWare Convert Tool המיושן עם Directory Service Migration Tool. Directory Service Migration Tool מאפשר להגר, מבלי לפגוע במקור, NetWare Binderies ו- NetWare Domain Services למסד נתונים לא-מקוון, ובכך לאפשר למנהלי מערכת למדל את נתוני החשבון, לפני העברתו ל-Active Directory, כפי שמוצג בתרשים 3.1 (גישה מ- Windows 2000 ל-Novell).



תרשים 3.1 הגירה מ- NetWare Domain Services ל- Active Directory של Windows 2000

- **File and Print Services for NetWare.** שירותים אלה מאפשרים ללקוחות NetWare המשתמשים בתעבורה תואמת-IPX/SPX לשלוח עבודות הדפסה לשרתי הדפסה של Windows 2000. שירות זה הוא שירות נפרד מ- Windows 2000 ואינו דורש עריכת שינויים כלשהם בלקוחות NetWare (גישה מ-Novell ל- Windows 2000).

שילוב שרתי NetWare 5.0 עם שרתי Windows 2000

כמו Windows 2000, כך גם NetWare גירסה 5.0 משתמשת בפרוטוקול TCP/IP כפרוטוקול הטבעי שלה, וכברירת מחדל פרוטוקול IPX אינו מותקן. לא Client Service for NetWare ולא Gateway Service for NetWare תומכים בהתחברות למשאבי NetWare באמצעות IP. בשל כך, כאשר אתה משתמש ב-NWLink להתחברות לשרתי NetWare 5.0, חובה עליך לאפשר IPX בשרתים אלה.

NWLink ו- Windows 2000

NWLink מספק את פרוטוקולי הרשת והתעבורה לתמיכה בהתקשרויות עם שרתי קבצים של NetWare, ויש להתקין אותו אם אתה מעוניין להשתמש ב- Gateway Service for NetWare או ב- Client Service for NetWare כדי להתחבר לשרתי NetWare. כדי להתחבר לרשת NetWare באמצעות מחשב מבוסס Windows 2000 Professional, עליך להשתמש ב- Client Service for NetWare או לקוח NetWare של צד-שלישי, כגון Novell Client for Windows 2000. לחילופין, תוכל להשתמש בפתרון מבוסס Gateway, על ידי התקנת Gateway Service for NetWare בשרת Windows 2000. בהמשך הפרק יתקיים דיון מורחב בנושא Gateway Service for NetWare ו- Client Service for NetWare.

מכיון ש-NWLink הוא מותאם NDIS ‏(NDIS-Compliant, **N**etwork **D**river **I**nterface **S**pecification-Compliant), יכול מחשב מבוסס Windows 2000 להפעיל במקביל מחסניות פרוטוקול אחרות, כגון TCP/IP. ‏NWLink יכול להתאגד למספר כרטיסי רשת במיגוון סוגי מסגרות (Frame Types). ‏NWLink דורש מעט מאוד, אם בכלל, הגדרות בלקוח ברשתות קטנות ושאינן מנותבות.

הערת המתרגם התרגום במילון למילה Compliant הוא **מתרצה**, **נעתר**, **מוותר**. בהקשר המילה לתחום המחשבים הפכה המילה להיות **מותאם**, כמו לדוגמה Year 2000 Compliant Software/Hardware, תוכנה/חומרה המותאמת לבאג 2000 הידוע לשימצה, שבסופו של דבר גרם לנזק קטן ביותר.

NetBIOS ו- Windowss Sockets

NWLink תומכת בשני ממשקי תכנות ליישומי רישות (APIs) : NetBIOS ו- Windows Sockets (WinSock). ‏API אלה מאפשרים למחשב מבוסס Windows 2000 לתקשר עם לקוחות ושרתי NetWare, ועם כל מחשב מבוסס Windows המשתמש ב-NWLink. מכיון ש-NWLink תומך ב-NetBIOS הוא מאפשר התקשרות עם כל היישומים מבוססי-NetBIOS, כולל Microsoft System Management Server, שרת SNA, שרת SQL ושרת Exchange. ממשק WinSock ל-NWLink מאפשר ללקוחות מבוססי Windows בהם מותקן רק NWLink להשתמש ביישומים מבוססי WinSock, כגון Internet Explorer.

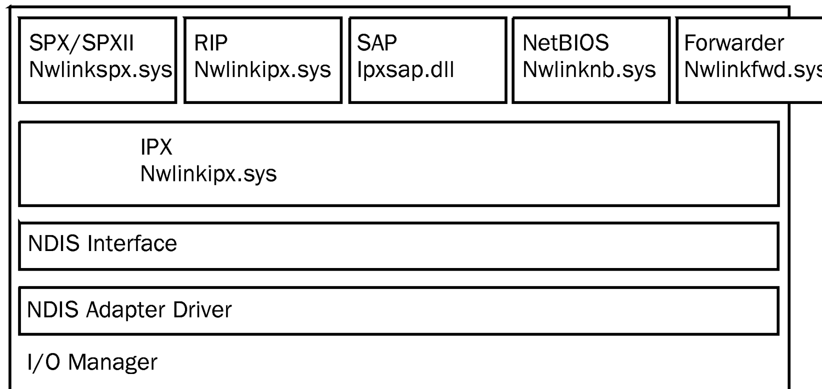
ארכיטקטורת NWLink

NWLink מספק ערכה כוללת של פרוטוקולי שכבת תעבורה ורשת המאפשרים שילוב עם סביבת NetWare. טבלה 3.1 מציגה רשימה של פרוטוקולי משנה ורכיבים, ומציגה את פעילותם ואת מנהלי ההתקן המשויכים אליהם.

טבלה 3.1 פרוטוקולי משנה של NWLink

פרוטוקול	פעילות	מנהל התקן
IPX	פרוטוקול רישות Peer-to-Peer המספק שירותים חסרי-חיבור להעברת צרורות נתונים ושולט במיעון וניתוב מנות נתונים בתוך ובין רשתות.	NWLNKIPX.SYS
SPX ו-SPXII	מספק שירותי העברה מוכווני-חיבור.	NWLNKSPX.SYS
RIP ‏(**R**outing **I**nformation **P**rotocol)	מספק שירותי גילוי של נתבים ונתיבים.	NWLNKIPX.SYS
SAP ‏(**S**ervice **A**dvising **P**rotocol)	אוסף ומפיץ שמות וכתובות של שירותים.	NWLNKIPX.SYS
NetBIOS	מספק תמיכה תואמת NetBIOS עבור IPX/SPX.	NWLNKNB.SYS
Forwarder	מספק תמיכה בנתב IPX.	NWLNKFWD.SYS

תרשים 3.2 מראה את NWLink בארכיטקטורת Windows 2000, ואת הקבצים בהם מיושם כל פרוטוקול.



תרשים 3.2 NWLink בארכיטקטורת Windows 2000

IPX

IPX הוא פרוטוקול Peer-to-Peer המספק שירותים Connectionless להעברת צרורות נתונים ושולט במיעון וניתוב מנות נתונים בתוך ובין רשתות. כאשר מדובר בהעברה Connectionless, אין צורך ליצור Session בכל פעם שמועברות מנות; המנות פשוט נשלחות לדרכן. דבר זה יוצר עומס נמוך יותר מאשר העברה Connection-Oriented, בה יש ליצור Session בכל פעם שמועברות מנות. בשל כך, העברה Connectionless יעילה יותר במקרים בהם המידע נוצר לסירוגין, ובהתקפים קצרים.

מכיון ש-IPX הוא פרוטוקול Connectionless, הוא אינו מספק לתחנה השולחת בקרת זרימה, או אישור לכך שצרור הנתונים התקבל כהלכה בתחנת היעד. במקום זאת, מנות נתונים יחידות נעות באופן עצמאי לכיוון יעדן, ו-IPX מניח שהן הגיעו שלמות, מבלי להבטיח שהן מגיעות ליעדן או שהן הגיעו ברצף. אבל, מכיון שההעברה ברשת LAN היא בטוחה משגיאות, באופן יחסי, IPX הוא פרוטוקול יעיל למשלוח כמויות קטנות של נתונים ב-LAN.

NWLink מאפשר תכנות יישומים עבור WinSock ועבור RPC over WinSock (**R**emote **P**rocedure **C**all over WinSock). IPX תומך במזהי WinSock (WinSock Identifications) לשימושים של יישומי WinSock. IPX מאפשר NetBIOS, Named Pipes, Mailslots, NetDDE (**Net**work **D**ynamic **D**ata **E**xchange), RPC over NetBIOS וגם RPC over Named Pipes Programming over NetBIOS over IPX (NBIPX). NWLink תומך גם ביישומים אחרים המשתמשים ב-IPX באמצעות אירוח ישיר (Direct Hosting). אירוח ישיר הוא תכונה המאפשרת למחשבים לתקשר באמצעות IPX, ולעקוף על ידי כך את שכבת NetBIOS. אירוח ישיר עשוי להפחית את התקורה ולהגביר את קצב ההעברה.

SPX

SPX הוא פרוטוקול תעבורה המציע שירותים Connection-Oriented על IPX. למרות ששירות Connection-Oriented דורש את התקורה של יצירת Session, מרגע שנוצר ה- Session, שירות זה אינו מעמיס על הרשת לצורך העברת נתונים יותר מאשר העומס שיוצר שירות Connectionless. בשל כך, הוא פועל היטב עם תוכניות שירות הדורשות חיבור מתמשך. SPX מספק שליחה בטוחה באמצעות סידור ומתן אישור (Acknowledgement), ומוודא שליחה מוצלחת של מנות לכל יעד, על ידי בקשת אישור (Verification) מהיעד ברגע קבלת הנתונים. אישור SPX חייב לכלול ערך התואם לערך שחושב מהנתונים לפני שליחתם. על ידי השוואת ערכים אלה מבטיח SPX לא רק שהמנה הגיעה ליעדה, אלא גם שהיא הגיעה בשלמותה. SPX יכול לעקוב אחר העברות נתונים הכוללות סדרות של מנות נפרדות. אם בקשה לאישור (Acknowledgement Request) אינה גורמת לתגובה בתוך זמן מוגדר, SPX חוזר ושולח את הבקשה, עד שמונה פעמים. אם לא התקבלה תגובה כלשהי, מניח SPX כי התרחש כשל בחיבור.

SPX גם מספק מנגנון התפרצות מנות (Packet Burst Mechanism). התפרצות מנות, המוכר גם כמצב התפרצות (Burst Mode), מאפשר העברת מספר מרובה של מנות נתונים מבלי שיידרש אישור קבלה וארגון בסדרה של כל אחת מהן בנפרד. על ידי אפשור קבלת אישור קבלה (Acknowledge) יחיד, יכול מצב ההתפרצות להפחית את העומס על הרשת ברוב הרשתות מבוססות IPX. יתר על כן, מנגנון התפרצות המנות מנטר מנות פגומות ומשדר פעם נוספת רק אותן. ב-Windows 2000 מצב התפרצות מאופשר כברירת מחדל.

SPXII

SPXII מהווה שיפור של SPX בכך שהוא מאפשר לו לפעול ברשתות בעלות פס רחב הרבה יותר. השיפורים יימצאו בנקודות הבאות:

- **SPXII מאפשר לצפות ליותר מאשר אישור קבלה אחד, כפי שהדבר ב-SPX.** ב-SPX, לא ייתכן מצב בו תהיה יותר ממנה אחת שלא קיבלה אישור קבלה. לעומת זאת, ב-SPXII יכול להיווצר מצב בו יותר ממנת נתונים אחת עדיין לא קיבלה אישור קבלה. מספר המנות האפשרי למנות הממתינות לאישור קבלה בעת העבודה עם SPXII נקבע בין עמיתים ברשת בעת הקמת החיבור ביניהם.
- **SPXII מאפשר מנות גדולות יותר.** SPX מאפשר מנת נתונים בגודל מירבי של 576 בתים (576-bytes), בו בזמן שגודלה המירבי של מנת נתונים ב-SPXII הוא הגודל המירבי שנקבע עבור סוג ה-LAN עליה הוא פועל. לדוגמה, ברשת Ethernet יכול SPXII להשתמש במנה בגודל 1518 בתים (1518-bytes).

RIP

NWLink משתמש ב-RIP over IPX (**R**outer **I**nformation **P**rotocol over IP**X**, RIPX) כדי ליישם שירותי נתיב וגילוי נתיבים בהם משתמשים SPX ו- NBIPX. RIP שולח ומקבל תעבורת IPX ושומר טבלת ניתוב. RIP פועל בשכבה המקבילה לשכבת היישום (Application Layer) של מודל OSI. הקוד של RIP מיושם בקובץ מנהל ההתקן NWLNKIPX.SYS.

NWLink כולל את פרוטוקול RIP עבור לקוחות מבוססי-Windows ועבור מחשבים מבוססי Windows 2000 Server בהם לא מותקן Routing and Remote Access Service. מחשבים אלה אינם מעבירים מנות כפי שעושים זאת נתבים, אך הם משתמשים בטבלת RIP כדי לקבוע להיכן עליהם לשלוח את המנות. לקוחות RIP, כגון תחנות עבודה, יכולים לזהות את הנתיב האופטימלי למספר רשת IPX על ידי Broadcast בקשת ניתוב GetLocalTarget של RIP. כל נתב שיכול להגיע אל היעד מגיב לבקשה זו עם נתיב יחיד. בהתאם לתגובות RIP מהנתבים המקומיים, בוחרת התחנה השולחת את הנתב הטוב ביותר באמצעותו היא תעביר את מנות IPX שלה.

SAP

SAP (**S**ervice **A**dvertising **P**rotocol) הוא המנגנון באמצעותו אוספים ומפיצים לקוחות IPX את השמות והכתובות של השירותים הפועלים בצמתי IPX. לקוחות SAP משתמשים בשידורי SAP רק כאשר כשלו שאילתות מבוססות Bindery או NDS (**N**etWare **D**omain **S**ervices). לקוחות SAP שולחים את הסוגים הבאים של הודעות:

- לקוחות SAP מבקשים את השם והכתובת של השרת הקרוב ביותר מסוג מסוים, על ידי שידור רחב של בקשת GetNearestServer של SAP.
- לקוחות SAP מבקשים את שמותיהם וכתובותיהם של כל השירותים, או כל השירותים מסוג מסוים, על ידי שידור רחב של בקשת שירות כללי (General Service Request) של SAP.

NWLink כולל ערכת משנה של פרוטוקול SAP עבור לקוחות מבוססי-Windows ועבור מחשבים מבוססי Windows 2000 Server בהם לא מותקן נתב IPX.

NetBIOS over IPX

כדי להקל על פעולתם של יישומים מבוססי-NetBIOS ברשת IPX, מספק NetBIOS over IPX (NWLNKNB.SYS) שירותי NetBIOS תקניים כגון אלה:

- **NetBIOS Datagram Services.** יישומים משתמשים ב- NetBIOS Datagram Services לצורך תקשורת Connectionless מהירה. Mailslots ואימות משתמשים בשירות זה.
- **NetBIOS Session Services.** מספק תקשורת Connection-Oriented אמינה בין יישומים. שיתוף קבצים והדפסות מסתמך על שירות זה.
- **NetBIOS Name Service.** ניהול שמות, כולל רישום, שאילתה ושחרור שמות NetBIOS.

Forwarder

Forwarder הוא רכיב מצב ליבה (Kernel Mode) אשר מותקן יחד עם NWLink. אבל, נעשה בו שימוש רק כאשר שרת מבוסס-Windows 2000 משמש כנתב IPX המפעיל את Routing and Remote Access Service.

כאשר מופעלת תוכנת ניתוב IP, פועל רכיב Forwarder עם IPX Router Manager ועם רכיב הסינון כדי להעביר מנות. רכיב Forwarder משיג את נתוני ההגדרה מ- IPX Route Manager ומאחסן טבלה ובה הנתיבים הטובים ביותר. כאשר הרכיב Forwarder מקבל מנה נכנסת הוא מעביר אותה למנהל התקן המסנן, כדי לבחון אם קיימים בה מסנני קלט (Input Filters). כאשר הוא מקבל מנה יוצאת, קודם כל, הוא מעביר אותה למנהל התקן המסנן. בהנחה שלא קיים מסנן המונע מהמנה מלהישלח, מעביר רכיב הסינון את המנה חזרה והרכיב Forwarder מעביר אותה לממשק המתאים.

סיכום שיעור

NWLink הוא יישום 32 סיביות של Microsoft לפרוטוקול IPX/SPX. IPX הוא פרוטוקול רישות Peer-to-Peer המספק שירותי העברת צרורות נתונים Connectionless, ומבקר מיעון וניתוב של מנות. SPX הוא פרוטוקול תעבורה המציע שירותים Connection-Oriented על IPX. רכיב Forwarder פועל יחד עם IPX Router Manager ועם רכיב הסינון, כדי להעביר מנות בנתיב הטוב ביותר.

שיעור 2: שימוש ב-
Gateway Service for NetWare

Gateway Service for NetWare מאפשר ללקוח רישות של Microsoft (LAN Manager, MS-DOS, Windows for Workgroups, Windows 9x/NT/2000) לקבל גישה לשירותי שרת NetWare דרך מחשב מבוסס- Windows 2000 Server. בשיעור זה תלמד כיצד להתקין ולהגדיר את Gateway Service for NetWare.

לאחר שיעור זה, תוכל

- להתקין את Gateway Service for NetWare.
- לאפשר ולהפעיל Gateway בסביבת Windows 2000.

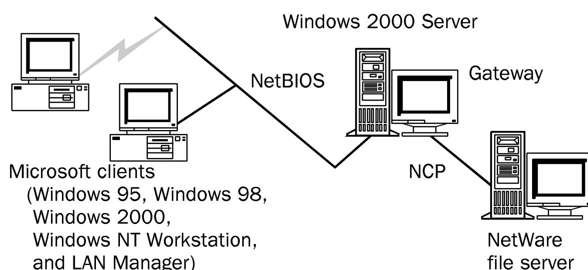
זמן לימוד משוער: 30 דקות

סקירת Gateway Service for NetWare

Gateway Service for NetWare מאפשר לך ליצור Gateway דרכו יוכלו מחשבי לקוח של Microsoft, בהם לא מותקנת תוכנת הלקוח של NetWare של Novell, לגשת למשאבי קבצים והדפסה של NetWare. תוכל ליצור Gateways למשאבים הממוקמים בעצים של NDS של Novell, כמו גם למשאבים בשרתים המפעילים אבטחת Bindery. משאבים אלה כוללים Volumes, Directories, אובייקטי מפת ספריה (Directory Map Objects), מדפסות (Printers) ותורי הדפסה (Print Queues). משתמש העובד באופן מקומי עם מחשב מבוסס Windows 2000 Server יכול להשתמש ב- Gateway Service for NetWare כדי לקבל גישה ישירה למשאבי קבצים והדפסה של NetWare, בין אם הם ב-NDS Tree ובין אם הם בשרתים בהם פועלת אבטחת Bindery. Gateway Service for NetWare סומך ופועל עם NWLink.

הבנת Gateway Service for NetWare ו-Gateways

Gateway Service for NetWare פועל כ-Gateway בין פרוטוקול NetBIOS, המשמש ברשת Windows, לבין NetWare Core Protocol, המשמש רשתות NetWare. כאשר Gateway מאופשר, לקוחות רשת הפועלים בסביבת Microsoft יכולים לגשת לקבצי ומדפסות NetWare, מבלי שיצטרכו להפעיל תוכנת לקוח באופן מקומי. תרשים 3.3 מציג דוגמה להגדרת שער קבצים (File Gateway).



תרשים 3.3
הגדרת File Gateway

לשם גישה לקובץ, שרת ה-Gateway מפנה את אחד מהכוננים שלו ל- NetWare Volume ואז משתף כונן זה עם לקוחות Microsoft האחרים. Files Gateway משתמש בחשבון NetWare במחשב המפעיל Windows 2000 Server, כדי ליצור חיבור מאומת לשרת NetWare. חיבור זה מופיע במחשב Windows 2000 Server ככונן מופנה (Redirected Drive). כשאתה משתף את הכונן המופנה הוא הופך להיות כמו כל משאב משותף אחר במחשב Windows 2000 Server.

לדוגמה, נניח שאתה מעוניין ליצור Gateway ממחשב AIREDALE (המפעיל Gateway Service for NetWare) לתיקיית NDS ב-Volume ששמו \\NW4\Server1\Org_Unit.Org\Data בשרת NetWare ששמו Nw4. כאשר תפעיל את ה-Gateway תציין את \\NW4\Server1\Org_Unit.Org\Data כמשאב NetWare, ואז תציין שם שיתוף עבור לקוחות Microsoft, כגון Nw_Data. מרגע זה ואילך, יתייחסו לקוחות Microsoft למשאב זה כאל \\AIREDALE\Nw_Data.

לאחר שנוצר החיבור ל-Gateway הוא מנותק רק במקרה והמחשב הפועל בסביבת Windows 2000 Server מכובה, או אם המנהל שלו (Administrator) מנתק את השיתוף או מבטל את ה-Gateway, או במקרה ותקלת רשת מונעת גישה לשרת NetWare. התנתקות (Logging Off) לכשעצמה מהמחשב הפועל בסביבת Windows 2000 Server אינה גורמת לניתוק ה-Gateway.

הערה מכיון שבקשות מלקוחות Microsoft מעובדות דרך ה-Gateway, הגישה איטית יותר מאשר גישה ישירה באמצעות לקוח NetWare. לקוחות המבקשים גישה למשאבי NetWare לעיתים קרובות צריכים להפעיל תוכנת לקוח של NetWare, כדי לקבל ביצועים טובים יותר.

התקנת Gateway Service for NetWare

כאשר תתקין את Windows 2000 Server תעמוד בפניך גם האפשרות להתקין את Gateway Service for NetWare. תוכל לעשות זאת בשלב מאוחר יותר, כאשר תתקין את GSNW. כדי להתקין ולהגדיר את Gateway Service for NetWare, עליך להיות מחובר למערכת בחשבון החבר בקבוצת המנהלים (Administrators Group). אם אתה מעוניין להתקין את Gateway Service for NetWare לאחר שכבר התקנת את Windows 2000 Server, פעל כך:

➤ **להתקנת Gateway Service for NetWare**

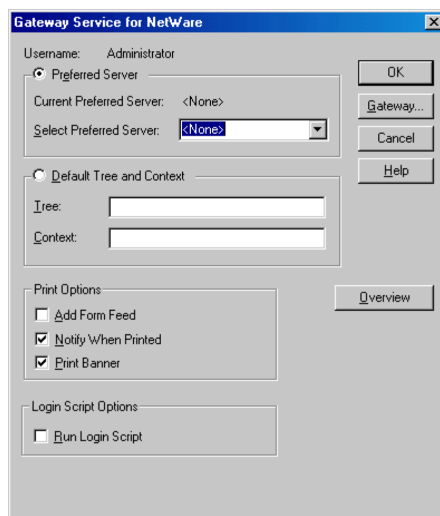
1. פתח את יישומון לוח הבקרה Network and Dial-Up Connections.
2. לחץ לחיצה ימנית על הסמל Local Area Connection, ומתפריט הקיצור בחר Properties.
3. בכרטיסיה General לחץ על Install.
4. בתיבת דו-שיח Select Network Component Type, לחץ על Client, ולחץ על Add.
5. בתיבת דו-שיח Select Network Client, לחץ Gateway (and Client) Service for NetWare, ולחץ OK.

אם בעת התקנת Gateway Service for NetWare בשרת לא מאותרת התקנה של NWLink, הוא מותקן באופן אוטומטי. בנוסף, בעת התקנת Gateway Service for NetWare מותקן גם Client Service for NetWare ולחלון לוח הבקרה נוסף הסמל של Gateway Service for NetWare. כברירת מחדל מועברת רשת NetWare לראש סדר החיפוש ברשת (Network Search Order).

חשוב לפני שתתקין את Gateway Service for NetWare במחשב, הסר ממנו כל התקנה קיימת של תוכנת לקוח התואמת ל- NetWare Core Protocol, כולל תוכנת הלקוח של NetWare.

הגדרת Gateway Service for NetWare

בכניסה הראשונה למערכת לאחר התקנת Gateway Service for NetWare אתה מתבקש להגדיר את Default Tree and Context, או את השרת המועדף עליך. ה- Tree וה-Context מגדירים את מיקום אובייקט המשתמש עבור שם המשתמש בו אתה משתמש כדי להיכנס (Log on) ל-NDS Tree של Novell. שרת מועדף הוא שרת NetWare אליו אתה מתחבר באופן אוטומטי כאשר אתה נכנס לרשת שלך, אם הרשת שלך אינה משתמשת ב-NDS. כאשר אתה מתחבר ל-NetWare גירסה 4 ומעלה חובה עליך לציין Default Tree and Context, בעוד שבעת התחברות ל-NetWare גירסה 3 או קודמת עליך להשתמש בשרת המועדף. עליך להגדיר את Default Tree and Context רק בסביבת NDS של Novell; אחרת, תוכל לקבוע שרת מועדף. תרשים 3.4 מציג את תיבת הדו-שיח Gateway Service for NetWare.



תרשים 3.4 תיבת דו-שיח Gateway Service for NetWare

➢ כדי לקבוע שרת מועדף

1. לחץ Start, הצבע על Settings, לחץ על Control Panel. לחץ לחיצה כפולה על Gateway Service for NetWare.
2. לחץ על Preferred Server ובתיבה Select Preferred Server הקלד את השרת המועדף.

אם אינך מעוניין לקבוע שרת מועדף, לחץ None. אז תהיה מחובר לשרת NetWare הזמין הקרוב ביותר, והעבודה שלך עם רשת NetWare תתבצע מול שרת זה. אם לא תקבע שרת מועדף תתבקש להגדיר כזה בכל פעם שתיכנס למערכת (Log on).

ניתן להגדיר Default Tree and Context, או שרת מועדף, אך לא שניהם (בסביבת NDS של Novell אתה מגדיר Default Tree and Context). אם אתה בוחר Default Tree and Context, אתה עדיין יכול לגשת לשרתים בהם פועלת אבטחת Bindery.

➢ כדי לקבוע Default Tree and Context

1. לחץ Start, הצבע על Settings, לחץ על Control Panel. לחץ לחיצה כפולה על Gateway Service for NetWare.
2. לחץ על Default tree and context, ובתיבה Tree and Context הקלד את ה-Tree וההקשר.

יצירת Gateway

לפני שתוכל ליצור Gateway למשאבי NetWare, צריך שבשרת תהיה קבוצה בשם NTGATEWAY וחשבון משתמש לו יש את ההרשאות המתאימות עבור המשאבים אליהם אתה מעוניין לגשת. חשבון המשתמש של NetWare בו תשתמש חייב להיות חבר בקבוצה NTGATEWAY.

חשבון המשתמש של NetWare באמצעותו אתה מאפשר Gateways יכול להיות חשבון Novell NDS או חשבון Bindery. אם לשרת יהיו Gateways הן למשאבי NDS והן למשאבים המאוחסנים במחשבים המפעילים אבטחת Bindery, חשבון המשתמש חייב להיות חשבון Bindery (חשבון זה יכול להתחבר למשאבי NDS של Novell באמצעות הדמיית Bindery). אם אתה יוצר Gateway רק למשאבי NDS, יכול חשבון המשתמש להיות חשבון NDS.

אפשור Gateways בסביבת Windows 2000

יצירת Gateway היא פעולה של שני שלבים. ראשית, עליך לאפשר Gateways במחשב הפועל בסביבת Windows 2000 Server. כשאתה מאפשר Gateways, עליך להקליד את השם והסיסמה של חשבון המשתמש לו יש גישה לשרת NetWare, ושהוא גם חבר בקבוצה NTGATEWAY בשרת NetWare. עליך לבצע פעולה זו פעם אחת בלבד בכל מחשב אשר יתפקד כ-Gateway.

➢ כדי לאפשר Gateway בשרת

1. לחץ Start, הצבע על Settings, לחץ Control Panel, ולחץ לחיצה כפולה על Gateway Service for NetWare.
2. לחץ על Gateway, וסמן את תיבת הסימון Enable Gateway.
3. בתיבה Gateway Account הקלד את שם חשבון ה-Gateway שלך.
4. בתיבות Password ו- Confirm Password הקלד את הסיסמה של חשבון ה-Gateway.
כעת באפשרותך לשתף משאבי קבצים והדפסה של NetWare ברשת מבוססת-Windows.

הפעלת Gateways

הצעד השני בו עליך לנקוט הוא הפעלת ה-Gateway עבור כל Volume או מדפסת אליהם אתה מעוניין ליצור את ה-Gateway. כאשר אתה מפעיל Gateway, אתה מציין את משאב NetWare ושם השיתוף בהם ישתמשו לקוחות Windows כדי להתחבר למשאב זה. כדי להפעיל Gateway עבור Volume, היעזר ביישומון לוח הבקרה Gateway Service for NetWare. כדי להפעיל Gateway עבור מדפסת, היעזר באשף Add Printer. אם אתה מפעיל Gateway למשאב NDS של Novell, וחשבון המשתמש של ה-Gateway הוא חשבון Bindery, ציין את המשאב אשר משתמש ב- Bindery Context Name. אם אתה משתמש בחשבון משתמש של NDS, ואינך מתכוון ליצור Gateways גם למשאבי Bindery, ציין את שם משאב ה-NDS.

➢ כדי להפעיל Gateway עבור משאבי קבצים של NetWare

1. לחץ Start, הצבע על Settings, לחץ Control Panel, ולחץ לחיצה כפולה על Gateway Service for NetWare.
2. לחץ על Gateway, וסמן את תיבת הסימון Enable Gateway.
3. לחץ Add, ובתיבה Share Name הקלד את שם השיתוף בו ישתמשו לקוחות Microsoft לשם גישה למשאבי NetWare.
4. בתיבה Network Path הקלד את נתיב הרשת של NetWare Volume או הספריה אותם אתה מעוניין לשתף.
5. בתיבה Use Drive הקלד את אות כונן ברירת המחדל בה יש להשתמש, אם יש צורך בכך.
6. לחץ על Unlimited ולחץ OK.

ניתן גם ללחוץ על Allow, להקליד את מספר המשתמשים הבו-זמניים המותר ואז ללחוץ על OK.

➢ כדי להפעיל Gateway למדפסות NetWare

1. לחץ Start, הצבע על Settings, לחץ Printer.
2. לחץ Add Printer, ולחץ Next.
3. לחץ Network Printer, ולחץ Next.
4. בתיבה Name הקלד את שם המדפסת, על פי התחביר הבא:

\\servername\sharename

כדי לאתר מדפסת NetWare ב- Shared Printers, לחץ Next. אם יש צורך בכך, לחץ לחיצה כפולה על שמות ב-NDS Tree ושמות שרתי NetWare, עד שתאתר את המדפסת המבוקשת.

עקוב אחר ההוראות הנותרות באשף Add Printer כדי לסיים את ההתחברות למדפסת NetWare:

1. סמל המדפסת מופיע בחלון התיקיה Printers.
2. לחץ על המדפסת שזה עתה יצרת, פתח את תפריט File, ובחר Properties.
3. בכרטיסיה Share לחץ על Shared, ובתיבת דו-שיח Share As הקלד שם עבור המדפסת.

אבטחת משאבי Gateway

אבטחה עבור משאבי Gateway מסופקת בשתי רמות :

- במחשב הפועל בסביבת Windows 2000 Server והמשמש כ-Gateway, תוכל להגדיר הרשאות ברמת השיתוף (Share-level Permissions) עבור כל משאב הזמין דרך Gateway זה.
- בשרת קבצים של NetWare יכול מנהל הרשת (Administrator) לשייך זכויות נאמן (Trustee Rights) לחשבון המשתמש המשמש את ה-Gateway, או לקבוצה NTGATEWAY. זכויות אלו נאכפות על כל משתמשים שהם לקוחות Microsoft הניגשים למשאבים דרך ה-Gateway. לא קיימת ביקורת (Auditing) של גישה ל-Gateway .

התחברות ישירה למשאבי NetWare

בנוסף לכך שהוא מספק טכנולוגיית Gateway, מאפשר Gateway Service for NetWare למשתמשים העובדים באופן מקומי במחשב המפעיל Windows 2000 Server לגשת ישירות למשאבי NetWare, בדיוק כפי ש- Client Service for NetWare מאפשר זאת למשתמשים ב- Windows 2000 Professional. המידע בסעיף זה מתייחס למשתמשים העובדים באופן מקומי (Locally) במחשב בו פועלת מערכת ההפעלה Windows 2000 Server, אשר מבצע גישה ישירה למשאבי NetWare - לא ללקוחות Microsoft המבצעים את הגישה דרך Gateway (למרות האמור, מידע זה מתייחס גם למשתמשים המפעילים את Client Service for NetWare במחשבים בהם פועלת מערכת ההפעלה Windows 2000 Professional).

NDS Trees של Novell (כמו גם שרתי NetWare המפעילים אבטחת Bindery) מופיעים ברשימה NetWare או ברשימה Compatible Network של Windows Explorer (סייר Windows). תוכל ללחוץ לחיצה כפולה על שם Tree כדי לפרוש אותו, ואז ללחוץ לחיצה כפולה על כל אובייקט מכולה (Container Object), כדי להרחיב את תוכנו ואת מבנהו. תוכל להתחבר ולשייך כל אות כונן מקומי לכל Volume, תיקיה (Folder) או אובייקט מיפוי ספריה (Directory Map Object) בכל מקום בהיררכיית ה-Tree (אליו יש לך את האישורים). כדי להתחבר למדפסת NDS תוכל להיעזר באשף Add Printer, בדיוק כפי שאתה עושה לשם התחברות לכל מדפסת אחרת.

אם קבעת Default Tree and Context, לאחר שנכנסת למערכת (Logged on) אינך צריך להיכנס פעם נוספת או לספק שם משתמש או סיסמה אחרים כדי לגשת ל-Volume כלשהו ב- Default Tree שלך. אם תיגש ל-Tree אחר תתבקש לספק Context מלא (כולל שם משתמש) עבור Tree זה.

סיכום שיעור

Gateway Service for NetWare מאפשרים ללקוח רישות של Microsoft (LAN Manager, MS-DOS, Windows for Workgroups, Windows 9x/NT/2000) לגשת לשירותי שרת NetWare דרך Windows 2000 Server.

שיעור 3: שימוש ב-
Client Service for NetWare

לקוחות רשת Microsoft יכולים לגשת לשרת NetWare דרך שרת Windows 2000 בו פועל שירות Client Service for NetWare. מחשב מבוסס-Windows 2000 יכול לגשת למשאבים בשרת NetWare כלקוח, דרך הרכיב המשולב Client Service for NetWare. בשיעור זה תלמד כיצד להתקין ולהשתמש ב- Client Service for NetWare.

לאחר שיעור זה, תוכל

- להתקין Client Service for NetWare.
- לפרט את היתרונות והחסרונות בשימוש ב- Client Service for NetWare.

זמן לימוד משוער: 15 דקות

חיבוריות NetWare

Client Service for NetWare מספק חיבוריות NetWare מבוססת-לקוח, ואילו Gateway Service for NetWare מתפקד כ-Gateway דרכו מספר מרובה של לקוחות יכולים לגשת למשאבי NetWare. שניהם מסתמכים על ופועלים עם פרוטוקול NWLink, אשר מותקן באופן אוטומטי עם המנתב (Redirector). Client Service for NetWare משתמש בערכת משנה (Subset) של קוד Gateway Service for NetWare.

כאשר כונן ממופה ל-Volume NetWare, משתמש מחשב המפעיל את Windows 2000 Professional בחשבון NetWare כדי ליצור חיבור מאומת לשרת NetWare. לדוגמה, הוא ישמש ליצירת חיבור ממחשב A (בו פועל שירות לקוח, Client Service) ל-NDS Volume של Novell, \\T\Volname.Orgunit.Org\Folder, כאשר T הוא שם NDS Tree, Volname .Orgunit.Org הוא הנתיב לשם ה-Volume ב-NDS Tree ו- Folder הוא תיקיית המשנה ב-Volname Volume. בסייר Windows פתח את תפריט Tools, ולחץ על Map Network Drive. תוכל גם להשתמש בפקודת שורת הפקודה net use ולציין את הנתיב \\B\Volname.Orgunit.Org\Folder עבור שם משאב ה-NetWare. כאשר אתה משתמש בפקודת שורת הפקודה net use, לאחר שנוצר מיפוי הכונן, הוא מנותק רק במקרה והמחשב בו פועלת מערכת ההפעלה Windows 2000 Professional מכובה, אם מתבצע ניתוק ידני מכוון או אם תקלת רשת מונעת גישה לשרת NetWare. מיפוי הכונן מתחדש מייד עם כניסתו הבאה של המשתמש למערכת.

בחירה בין Client Service for NetWare לבין Gateway Service for NetWare

אם אתה מתכוון ליצור או לשמר עד אין קץ סביבה הטרוגנית המכילה שרתי Windows 2000 ושרתי NetWare, שקול את השימוש ב- Client Service for NetWare. אם אתה מתכוון להגר בהדרגה מסביבת NetWare לסביבת Windows 2000, או אם אתה מעוניין להפחית את עומס ניהול המערכת, שקול את השימוש ב- Gateway Service for NetWare.

יתרונות של Client Service for NetWare

Client Service מציג את היתרונות הבאים על פני Gateway Service :

- **Client Service מאפשר אבטחה ברמת המשתמש (User-level security), ולא ברמת השיתוף (Share-level Security).** Client Service for NetWare מאפשר למשתמשים שלך גישה לספריות הבית (Home Directory) של משתמשים (ספריות בהן מאוחסן מידע אישי של המשתמש) אשר מאוחסנות בכרכי NetWare. אז משתמשים יכולים למפות את ספריית הבית שלהם ו-Volumes נוספים אליהם יש להם גישה ברמת המשתמש. כדי לאפשר למשתמשים גישה לספריות בית דרך שירות השער (Gateway Service), עליך לספק לכל משתמש אות כונן שונה.
- **הביצועים של Client Service טובים מאלה של Gateway Service.** Client Service מתקשר ישירות עם שרתי NetWare, ונמנע על ידי כך מזמן אחזור (Latency) הנגרם על ידי המעבר דרך ה-Gateway אל שרת NetWare.

חסרונות של Client Service for NetWare

ל- Client Service החסרונות הבאים :

- **Client Service דורש ממך לנהל מספר חשבונות משתמשים עבור כל לקוח.** לכל לקוח עליך ליצור ולנהל בנפרד חשבון לקוח, הן עבור Windows 2000 והן עבור NetWare. אבל, אם תשתמש במוצר נוסף, כגון לקוח Novell עבור Windows 2000, לא תצטרך לעשות זאת. במערכת ההפעלה Windows NT 4.0, מבטל Directory Service Manager את הצורך ליצור חשבונות משתמשים נפרדים בשרתים מבוססי-Bindery.
- **Client Service גורם לעומס גבוה יותר של התקנה וניהול.** עם Client Service, עליך להתקין ולתחזק תוכנת שירות לקוח נוספת בכל מחשב Windows 2000 Professional.
- **Client Service דורש שתוסיף IPX לכל הרשת שלך.** שרתי Windows 2000 ושרתים הפועלים בסביבת NetWare 5.0 משתמשים בפרוטוקול TCP/IP כפרוטוקול הטבעי שלהם. אבל, Client Service דורש שתשתמש ב-IPX (באמצעות NWLink), ועשוי גם לדרוש אפשור ניתוב IPX בכל הרשת.

הגדרת Client Service for NetWare

כשאתה מתקין את Client Service for NetWare בסביבת Windows 2000 Professional, מותקן פרוטוקול התעבורה NWLink IPX/SPX/NetBIOS Compatible באופן אוטומטי. כדי להתקין את Client Service for NetWare צריכות להיות לך הרשאות מנהל (Administrator) למחשב בו מותקנת מערכת ההפעלה Windows 2000 Professional. ניתן להשתמש במצב התקנה אוטומטית (Unattended Setup Mode) לצורך הטמעות רחבות היקף של Windows 2000 Professional ושל Client Service for NetWare.

➢ להתקנת Client Service for NetWare

1. פתח את יישומון לוח הבקרה Network and Dial-Up Connections.
2. לחץ לחיצה ימנית על הסמל Local Area Connection לגביו אתה מעוניין להתקין את Client Service for NetWare, ומתפריט הקיצור בחר Properties.
3. בכרטיסיה General לחץ על Install.
4. בתיבת דו-שיח Select Network Component Type בחר Client, ולחץ Add.
5. בתיבת דו-שיח Select Network Client לחץ על Client Service for NetWare, ולחץ OK.

סיכום שיעור

Windows 2000 כוללת תוכנת לקוח התומכת בהתחברות לשרתים הפועלים בסביבת NetWare. עם Client Service for NetWare ב- Windows 2000 ועם Gateway Service for NetWare ב- Windows 2000 Server, יכולים משתמשים להשתמש במשאבי קבצים והדפסה הפועלים בשרתי NetWare.

שיעור 4: התקנת NWLink והגדרתו

בשיעור זה תלמד כיצד להתקין NWLink, אשר נכלל בכל מהדורות מערכת ההפעלה Windows 2000 לשם תמיכה בחיבוריות למחשבים הפועלים בסביבת NetWare ומערכות תואמות אחרות.

לאחר שיעור זה, תוכל

- להתקין את פרוטוקול NWLink ב- Windows 2000.
- להגדיר את פרוטוקול NWLink ב- Windows 2000.
- לזהות את מטרת סוג המסגרת ומספר הרשת.

זמן לימוד משוער: 30 דקות

Windows 2000 Professional וחיבוריות NetWare

Windows 2000 Professional נעזרת ב- Client Service for NetWare ובפרוטוקול NWLink כדי לאפשר חיבוריות בין Windows 2000 Professional לבין שרתי NDS או שרתים מבוססי-Bindery של Novell. NWLink הוא רכיב Windows המכיל את פרוטוקול IPX/SPX.

כאשר תשדרג מערכות מחשב ממערכות ההפעלה Windows 9x/NTW ל- Windows 2000 Professional תוכל להשאיר את Novell Client 32 המותקן בהן (אם מותקן). Windows 2000 Professional משדרגת מחשבים בהם פועל Novell Client 32 בגרסאות הקודמות לגירסה 4.7. בעת השדרוג ל- Windows 2000 Professional מותקן Novell Client 32 בגירסה 4.51. תהליך זה מאפשר שדרוג נקי גם של Novell Client 32, מבלי לפגום בתיפקודו. כדי להשיג את הגירסה המלאה של Novell Client for Windows 2000, עליך לפנות ישירות למפיץ מורשה של Novell.

הגדרת Client Service for NetWare

כשאתה מתקין את Client Service for NetWare בסביבת Windows 2000 Professional, מותקן פרוטוקול התעבורה NWLink IPX/SPX/NetBIOS Compatible באופן אוטומטי.

➢ **כדי להתקין את Client Service for NetWare**

1. פתח את יישומון לוח הבקרה Network and Dial-Up Connection.
2. לחץ לחיצה ימנית על סמל החיבור המקומי, שעבורו אתה מעוניין להתקין את Client Service for NetWare, ומתפריט הקיצור בחר Properties.
3. בכרטיסיה General לחץ על Install.
4. בתיבת דו-שיח Select Network Component Type לחץ על Client, ולחץ על Add.
5. בתיבת דו-שיח Select Network Clients לחץ על Client Service for NetWare, ולחץ OK.

הערה כדי להתקין Client Service for NetWare עליך להיות בעל הרשאות מנהל (Administrator) במחשב הפועל בסביבת Windows 2000 Professional.

התקנת פרוטוקול התעבורה NWLink IPX/SPX/NetBIOS Compatible

פרוטוקול NWLink אינו מותקן כברירת מחדל בעת התקנת Windows 2000, כפי שהדבר במקרה של TCP/IP. אבל, עומדת בפניך האפשרות להתקין את NWLink בעת ההתקנה, יחד עם פרוטוקולים נוספים, או שתוכל להתקין אותו בשלב מאוחר יותר.

➢ כדי להתקין NWLink

1. פתח את יישומון לוח הבקרה Network and Dial-Up Connection.
2. לחץ לחיצה ימנית על הסמל Local Area Connection, ובחר Properties.
3. בכרטיסיה General לחץ על Install.
4. בתיבת דו-שיח Select Network Component Type לחץ על Protocol, ולחץ על Add.
5. בתיבת דו-שיח Select Network Protocol לחץ על NWLink IPX/SPX/NetBIOS Compatible Transport Protocol, ולחץ OK.

כדי להיות בטוח ש-NWLink פועל כהלכה, במנחה שורת הפקודה הקלד את הפקודה ipxroute config. על המסך אמורה להופיע טבלה ובה מידע אודות האיגוד אליו מוגדר NWLink, כפי שניתן לראות בתרשים 3.5.

```
Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>ipxroute config

NWLink IPX Routing and Source Routing Control Program v2.00

Num  Name                          Network    Node            Frame
=====================================================================
1.   IpxLoopbackAdapter            1234cdef   000000000002    [802.2]
2.   Local Area Connection         00000000   00104b65146c    [802.2]
3.   NDISWANIPX                    00000000   c46820524153    [EthII] -

Legend
======
- down wan line

C:\>_
```

תרשים 3.5 מידע האיגוד של NWLink

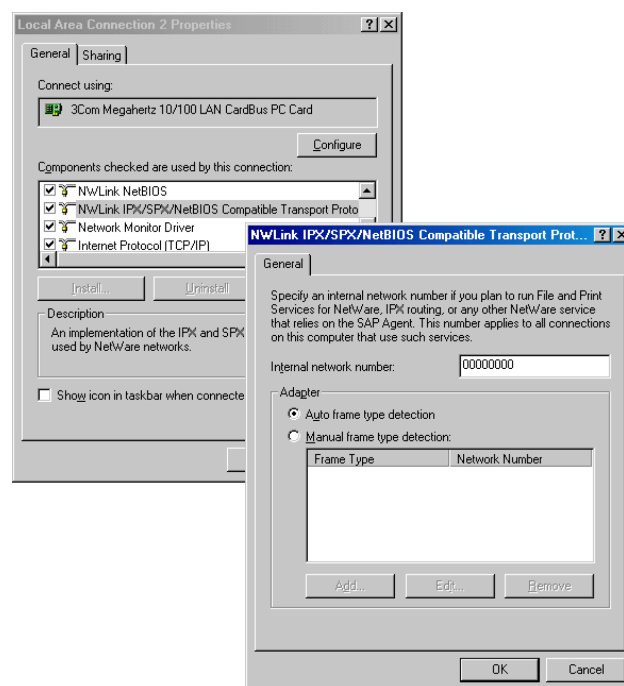
מספר רשת פנימי

מספר הרשת הפנימי משמש למטרות ניתוב פנימי, כשהמחשב הפועל בסביבת Windows 2000 מארח גם שירותי IPX. כשמחושב הנתיב הטוב ביותר להעברת מנות למחשב מסוים, ייתכן שיוצגו למחשבים מארחים מספר נתיבים להם אותה מטריקת נתיב, מה שעלול לגרום לחוסר בהירות איזה נתיב הוא הטוב ביותר. כשאתה מציין מספר רשת פנימי ייחודי, אתה יוצר רשת פנימית בתוך המחשב. הדבר מאפשר ניתוב אופטימלי מהרשת לשירותים הפועלים במחשב.

➢ כדי לשנות את מספר הרשת הפנימי

1. בלוח הבקרה לחץ לחיצה כפולה על Network and Dial-Up Connection.
2. לחץ לחיצה ימנית על הסמל Local Area Connection, ובחר Properties.
3. בכרטיסיה General לחץ על NWLink IPX/SPX/NetBIOS Compatible Transport Protocol ולחץ על Properties.
4. בתיבה Internal network number הקלד מספר, כפי שמוצג בתרשים 3.6, ולחץ OK.

הערה ככלל, אין צריך לשנות את מספר הרשת הפנימי.



תרשים 3.6 תיבת דו-שיח NWLink IPX/SPX/NetBIOS Compatible Transport Protocol

Frame Type ומספר רשת

סוג המסגרת (Frame Type) מגדיר את האופן בו מתאם הרשת, במחשב מבוסס Windows 2000, מרכיב את הנתונים לשליחה ברשת. כדי לתקשר בין מחשב הפועל בסביבת Windows 2000 ושרתי NetWare, עליך להגדיר את NWLink IPX/SPX/NetBIOS Compatible Transport Protocol (NWLink) במחשב Windows 2000 עם אותו Frame Type המשמש את שרתי NetWare. טבלה 3.2 מציגה רשימה של טופולוגיות ו- Frame Types הנתמכות על ידי NWLink.

טבלה 3.2 Frame Types של NWLink

סוג הרשת	סוגי Frames נתמכים
Ethernet	Ethernet II, 802.2, 802.3, 802.2 SNAP (SubNetwork Access Protocol)
Token Ring	802.5 ו- 802.5 SNAP
Fiber Distributed Data Interface	802.2 ו- SNAP

Frame Types מגדירים את מבנה הכותרת העליונה והתחתונה בהם משתמשים פרוטוקולי שכבת קישור הנתונים (Data-Link Layer) השונים.

בעת תהליך הזיהוי האוטומטי (Auto Detect), מנסה NWLink כל אחד מה- Frame Types הזמינים ברשימה עבור סוג מדיום הגישה המשויך. למשל, ברשת Ethernet ייערך ניסוי על Ethernet 802.2, Ethernet 802.3, Ethernet II וגם 802.2 SNAP (**S**ub**n**etwork **A**ccess **P**rotocol), כדי לבחון באמצעות איזה Frame Types יכול NWLink לתקשר. כאשר NWLink מקבל תגובה משרת NetWare לאחד מה- Frame Types הוא גם מקבל את מספר הרשת המשויך עם Frame Type עבור מקטע הרשת בו נמצא הלקוח. אז, מתאגד NWLink מחדש תוך שימוש ב- Frame Types עבורם התקבלה התגובה.

מספר הרשת החיצוני הוא מספר ייחודי המייצג מקטע רשת מסוים ו-Frame Type משויך. כל המחשבים באותו מקטע רשת, המשתמשים בסוג המסגרות האמור, חייבים שיהיה להם את אותו מספר רשת חיצוני, שחייב מצידו להיות ייחודי לכל מקטע רשת.

IPX Frame Type ומספר הרשת נקבעים בעת ההגדרה הראשונית של שרת NetWare. התכונה Auto Detect של NWLink מזהה את ה- Frame Type ומספר הרשת שהוגדרו בשרת(י) NetWare. Auto Detect של NWLink היא האפשרות המומלצת בבואך להגדיר מספר רשת ו-Frame Type.

מדי פעם קורה שהתכונה Auto Detect בוחרת מהמתאם שילוב לא נכון של מספר רשת ו-Frame Type. מכיון ש- Auto Detect נעזרת בתגובות שהיא מקבלת ממחשבים באותו מקטע רשת, היא עלולה לבחור את ה- Frame Type או את מספר הרשת הלא נכון, אם המחשבים מגיבים בערכים שגויים. הדבר עלול לקרות בעיקר במקרה של הגדרה ידנית שגויה באחד המחשבים האחרים ברשת. אם התכונה Auto Detect בוחרת Frame Type ומספר רשת שאינו מתאים למתאם המסוים, תוכל לקבוע באופן ידני את ה- Frame Type ואת מספר הרשת עבור מתאם מסוים זה. ה- Frame Type ומספר הרשת ב- Windows 2000 Professional חייב להתאים ל-Frame Type ומספר הרשת המוגדרים בשרת NetWare. תוכל לציין Frame Type ומספר רשת 00000000 כדי לאפשר זיהוי אוטומטי של מספר הרשת במקטע רשת זה.

➢ **כדי לשנות את מספר הרשת ואת ה- Frame Type**

1. פתח את יישומון לוח הבקרה Network and Dial-Up Connection.
2. לחץ לחיצה ימנית על הסמל Local Area Connection, ובחר Properties.
3. בכרטיסיה General לחץ על NWLink IPX/SPX/NetBIOS Compatible Transport Protocol ולחץ Properties.
4. בתיבת הרשימה הנפתחת Frame Type בחר את ה- Frame Type המתאים.
5. בתיבת הטקסט Network Number הקלד מספר רשת ולחץ OK.

אזהרה ברוב המקרים לא תצטרך לשנות את מספר הרשת ואת ה- Frame Type, מפני ש- Auto Detect אמורה לזהות נכון את ה- Frame Type ואת מספר הרשת. אם תבחר בהגדרות לא נכונות, לא יוכל הלקוח לתקשר עם שרתי NetWare.

כאשר קיים ברשת יותר מאשר Frame Type אחד עלינו להגדיר את מספרי הרשת באופן ידני, מכיון ש-NWLink מזהה רק Frame Type אחד באופן אוטומטי, ומתעלם מהשאר.

הגדרת NWLink

כדי להגדיר את NWLink, עליך להתקין את NWLink IPX/SPX/NetBIOS Compatible Transport Protocol ולהיות חבר בקבוצה Administrators. תוכל להיעזר בהליך הבא אם אתה מעוניין לאגד (Bind) NWLink למתאם רשת שונה, או כדי לשנות באופן ידני את ה- Frame Type.

➢ **כדי להגדיר את NWLink**

1. פתח את יישומון לוח הבקרה Network and Dial-Up Connection.
2. לחץ לחיצה ימנית על הסמל Local Area Connection, ובחר Properties.
3. בכרטיסיה General לחץ על NWLink IPX/SPX/NetBIOS Compatible Transport Protocol ולחץ Properties.
4. בכרטיסיה General הקלד ערך עבור Internal network number, או השאר את ערך ברירת המחדל 00000000 ללא שינוי.
5. אם אתה מעוניין ש- Windows 2000 Professional תבחר באופן אוטומטי את ה- Frame Type, לחץ על Auto Frame Type Detection ולחץ OK. דלג על שלבים 6 עד 10 בהליך זה.

   כברירת מחדל, NWLink מזהה באופן אוטומטי את ה- Frame Type המשמש את מתאם הרשת אליו הוא מאוגד. אם NWLink מזהה שאין תעבורה, או אם מזוהים מספר Frame Types, בנוסף ל-Frame Type 802.2, NWLink יקבע את ה- Frame Type לסוג 802.2.

6. כדי לקבוע באופן ידני את ה- Frame Type, לחץ על Manual Frame Type Detection.
7. לחץ Add.
8. בתיבת דו-שיח Manual Frame Detection בתיבה Frame Type, בחר את ה-Frame Type.

   תוכל לקבוע את מספר הרשת החיצוני, ה- Frame Type ומספר הרשת הפנימי בהם משתמשים הנתבים שלך על ידי הקלדת פקודה ipxroute config במנחה שורת הפקודה.
9. בתיבה Network Number הקלד מספר רשת, ולחץ Add.
10. חזור על צעדים אלה עבור כל Frame Type שאתה מעוניין לכלול, ולסיום לחץ OK.

תרגול: התקנת פרוטוקול NWLink

בתרגול זה תתקין ותגדיר את NWLink IPX/SPX/NetBIOS Compatible Transport Protocol. בנוסף, תשנה את סדר האיגוד של פרוטוקול NWLink.

➢ כדי להתקין ולהגדיר את NWLink

1. פתח את יישומון לוח הבקרה Network and Dial-Up Connection.
2. לחץ לחיצה ימנית על הסמל Local Area Connection, ובחר Properties.

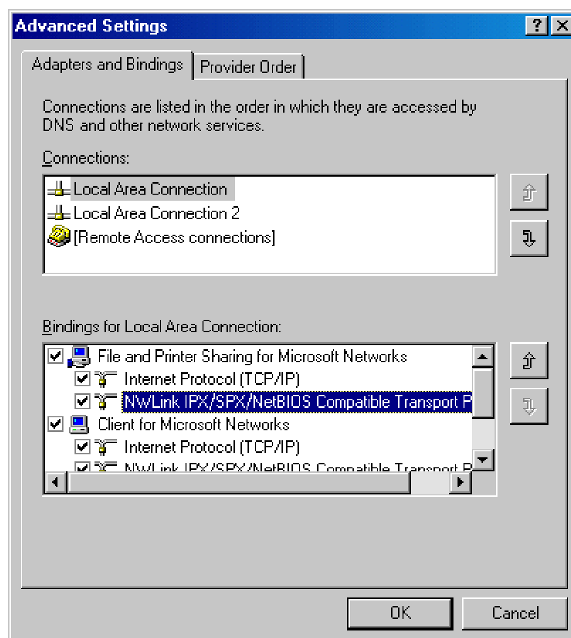
   נפתחת תיבת דו-שיח Local Area Connection Properties.
3. לחץ Add.

   מופיעה תיבת דו-שיח Select Network Component Type.
4. לחץ על Protocol ולחץ Add.
5. בחר NWLink IPX/SPX/NetBIOS Compatible Transport Protocol ולחץ OK.

   מופיעה תיבת דו-שיח Local Area Connection Properties.
6. בחר NWLink IPX/SPX/NetBIOS Compatible Transport Protocol, ולחץ Properties. בשלב זה תוכל לבחור בין זיהוי אוטומטי לזיהוי ידני של ה- Frame Type.

➢ כדי לשנות את סדר האיגוד של פרוטוקול NWLink

1. פתח את יישומון לוח הבקרה Network and Dial-Up Connection.
2. לחץ לחץ על חיבור הרשת אותו אתה מעוניין לשנות, פתח את תפריט Advanced, ובחר Advanced Settings.
3. בכרטיסיה Adapters and Binding בתיבה Binding for adapter name לחץ על NWLink Protocol, והעבר אותו כלפי מטה ברשימה על ידי לחיצה על החץ המורה כלפי מטה, כפי שנראה בתרשים 3.7.



תרשים 3.7 תיבת דו-שיח Advanced Settings

סיכום שיעור

IPX/SPX הוא מחסנית פרוטוקול המשמשת את רשתות Novell. פרוטוקול התעבורה NWLink IPX/SPX/NetBIOS Compatible מאפשר למחשבים מבוססי-Windows 2000 לתקשר עם רשתות Novell. כאשר אתה מתקין את Client Service for NetWare ב-Windows 2000 מותקן גם NWLink IPX/SPX/NetBIOS Compatible Transport Protocol באופן אוטומטי.

כדי להגדיר את NWLink, עליך להתקין את NWLink IPX/SPX/NetBIOS Compatible Transport Protocol ולהיות חבר בקבוצה Administrators. מספר הרשת הפנימי משמש למטרות ניתוב פנימי, כאשר מחשב הפועל בסביבת Windows 2000 מפעיל גם שירותי IPX. ה- Frame Type מגדיר את האופן בו מתאם הרשת, במחשב מבוסס-Windows 2000, מעצב את הנתונים לשליחה ברשת. מספר הרשת החיצוני הוא מספר ייחודי המייצג מקטע רשת מסוים ו-Frame Type המשויך לו. לכל המחשבים באותו מקטע רשת המשתמשים ב- Frame Type מסוים חייב להיות אותו מספר רשת חיצוני, אשר מצידו חייב להיות ייחודי לכל מקטע רשת.

שאלות סיכום

השאלות הבאות נועדו לחזק את הנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות על שאלה, עיין בשיעור המתאים ונסה את השאלה שנית. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואחר כך בעברית.

Answering the following questions will reinforce key information presented in this chapter. If you are unable to answer a question, review the appropriate lesson and then try the question again. Answers to the questions can be found in Appendix A, "Questions and Answers".

1. What is NWLink and how does it relate to Windows 2000?
2. What is SPX?
3. What is Gateway Service for NetWare?
4. When choosing between using Client Service for NetWare and Gateway Service for NetWare, what should you consider?
5. What is the NWLink Auto Detect feature?

1. מהו NWLink וכיצד הוא משפיע על Windows 2000?
2. מה זה SPX?
3. מה זה Gateway Service for NetWare?
4. כאשר עומדת בפניך אפשרות בחירה בין Client Service for NetWare לבין Gateway Service for NetWare, איזה שיקולים עליך לשקול?
5. מהי התכונה Auto Detect של NWLink?

פרק 4

ניטור פעילות רשת

אודות פרק זה

תקשורת ברשת הופכת להיות לנושא מרכזי בסביבת העבודה של היום. בדומה להתנהגות המעבדים וכונני הדיסקים במערכת שלך, להתנהגות הרשת יש השפעה על פעולת המחשב שלך. בפרק זה תלמד כיצד למטב את ביצועי המערכת שלך, על ידי ניתוח ביצועי הרשת, כגון ניטור תעבורת הרשת וניצול משאבים. מערכת ההפעלה Windows 2000 מספקת שתי תוכניות שירות עיקריות לניטור ביצועי הרשת. תוכניות שירות אלו הן System Monitor ו- Network Monitor. התוכנית System Monitor, המותקנת בעת התקנת Windows 2000 Professional ו- Windows 2000 Server, עוקבת אחר ניצול משאבים ותפוקת הרשת. התוכנית Network Monitor, שהיא רכיב אופציונלי עבור Windows 2000 Server, עוקבת אחר תפוקת הרשת במונחים של תעבורת רשת לכודה. פרק זה מתמקד בשימוש ב- Network Monitor לבדיקת תעבורה מקומית.

לפני שתתחיל

להשלמת פרק זה צריך שיהיה לך:

- שרת Windows 2000 מותקן.

שיעור 1: סקירת Network Monitor

תוכל להשתמש ב- Network Monitor של Windows 2000, כדי לצפות ולאתר בעיות ברשת המקומית (LAN). למשל, תוכל להשתמש ב- Network Monitor כדי לאבחן בעיות חומרה ותוכנה כאשר שניים (או יותר) מהמחשבים אינם מצליחים לתקשר ביניהם. תוכל גם להעתיק יומן (Log) של פעילות הרשת לקובץ, ואז לשלוח את הקובץ למומחה לניתוח רשתות, או למחלקת התמיכה. בנוסף, מפתחי יישומי רשת יכולים להיעזר ב- Network Monitor כדי לנטר ולאתר תקלות (Debug) ביישומי רשת בעת פיתוחם.

לאחר שיעור זה, תוכל

- להתקין את Network Monitor.
- לתאר את היתרונות שבשימוש ב- Network Monitor.

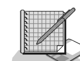
זמן לימוד משוער: 15 דקות

הבנת Network Monitor

תוכל להשתמש ב- Network Monitor כדי לאסוף מידע הנשלח אל ומאת מחשבים, ואז לסקור ולנתח מידע זה. Network Monitor לוכד מסגרות ומנות בשכבת קישור הנתונים (Data-link Layer) ומציג אותן באופן גרפי. מסגרות ומנות מורכבות מחלקיקים רבים של מידע, הכולל בין השאר:

- כתובות מקור ויעד
- נתוני סדרור (Sequencing)
- סכומי ביקורת (Checksums)

Network Monitor מפענח (Decode) מידע זה, ובכך מאפשר לך לנתח תעבורת רשת ולאתר תקלות רשת. בנוסף לנתוני שכבת קישור הנתונים, יכול Network Monitor גם לפענח חלק מנתוני שכבת היישום (Application Layer), כגון HTTP (**H**yper**T**ext **T**ransfer **P**rotocol) ו-FTP (**F**ile **T**ransfer **P**rotocol). נתונים אלה יכולים לסייע בידך לאתר תקלות בעסקאות של הדפדפן או של שרת האינטרנט.

 תרגול: התקנת Network Monitor

כדי שתוכל ללכוד, להציג ולנתח מסגרות רשת, עליך להתקין ב- Windows 2000 את Network Monitor ומנהל התקן הנקרא Network Monitor Driver. בתרגול זה תתקין את Network Monitor ב- Windows 2000 Server.

➢ **כדי להתקין את Network Monitor**

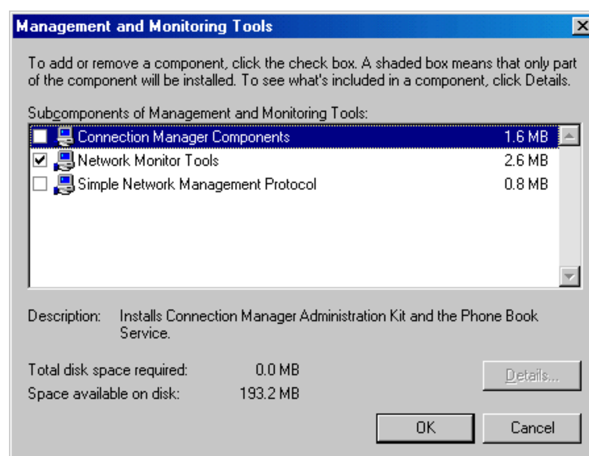
1. לחץ על Start, הצבע על Settings, ובחר Add/Remove Programs.
2. לחץ על Add/Remove Windows Components.

3. בחלון Windows Component Wizard סמן את Management and Monitoring Tools, ולחץ Details.

4. בתיבת דו-שיח Management and Monitoring Tools סמן את תיבת הסימון שליד Network Monitor Tools, כפי שמוצג בתרשים 4.1, ולחץ OK.

5. לחץ על NEXT בחלון Windows Component Wizard. אם תתבקש, הכנס את תקליטור ההתקנה המקורי של Windows 2000 Server לכונן התקליטורים או הקלד את נתיב הרשת בו נמצאים קבצי ההתקנה.

6. לחץ Finish להשלמת תהליך ההתקנה.



תרשים 4.1 בחירת רכיבי Network Monitor Tools

הערה Network Monitor מורכב מסוכן איסוף (Gathering Agent) אשר אוסף נתונים, ומתוכנית ניהול (Administrative Utility) המציגה ומנתחת נתונים אלה. התקנת Network Monitor Tools ב- Windows 2000 מתקינה באופן אוטומטי גם את הסוכן וגם את תוכנית הניהול של Network Monitor.

Network Monitor Driver

מנהל ההתקן של Network Monitor אוסף מסגרות ממתאם הרשת ומעביר את המידע לתוכנית השירות Network Monitor, לצפייה וניתוח. מנהל ההתקן (Driver) יכול גם להעביר מסגרות למנהל מרוחק המפעיל גירסה של Network Monitor הנכללת ב- SMS (**S**ystem **M**anagement **S**erver).

הערה כאשר אתה מתקין את מנהל ההתקן של Network Monitor נוסף גם האובייקט Network Segment, לשימושו של System Monitor.

התקנת מנהל ההתקן בלבד אינה מתקינה את תוכנית הניהול. אם אתה מעוניין לצפות ולנתח את נתוני Network Monitor במערכת, עליך להתקין את Network Monitor Tools במלואם במחשב הפועל בסביבת Windows 2000 Server.

➢ **כדי להתקין את מנהל ההתקן של Network Monitor**

1. פתח את יישומון לוח הבקרה Network and Dial-Up Connections.
2. לחץ לחיצה ימנית על סמל Local Area Connection אחריו אתה מעוניין לנטר, ומתפריט הקיצור בחר Properties.
3. בתיבת דו-שיח Local Area Connection Properties לחץ Install.
4. בתיבת דו-שיח Select Network Component Type לחץ על Protocol, ולחץ Add.
5. בתיבת דו-שיח Select Network Protocol לחץ על Network Monitor Driver, ולחץ OK.
   אם תתבקש, הכנס את תקליטור ההתקנה המקורי של Windows 2000, או הקלד את נתיב הרשת בו נמצאים קבצי ההתקנה.

לכידת נתוני רשת

Network Monitor נעזר בהליך הנקרא לכידה (Capturing) לבדיקת מסגרות רשת. תוכל ללכוד את כל תעבורת הרשת אל ומאת כרטיס הרשת המקומי, או ללכוד קבוצה מוגדרת של מסגרות. בנוסף, תוכל להגדיר את Network Monitor כך שיגיב לאירועים ברשת שלך. בשיעור 2 תלמד כיצד ללכוד ולנתח נתוני רשת.

סיכום שיעור

תוכל להיעזר ב- Network Monitor של Windows 2000 כדי לצפות ולנתח בעיות ברשת שלך. תוכל גם לאחסן בקובץ יומן (LOG) של פעילות רשת ולשלוח את הקובץ למנתח מערכות מומחה, או למחלקת התמיכה הטכנית.

שיעור 2: שימוש ב- Network Monitor

בשיעור זה תלמד כיצד להשתמש ב- Network Monitor לשם איתור תקלות ברשת. כאשר תשתמש ב- Network Monitor, עליך לזכור שתי נקודות עיקריות:

1. הפעל את Network Monitor בעת שפעילות הרשת נמוכה, או לפרקי זמן קצרים. הדבר יפחית את ההשפעה על ביצועי המערכת הנגרמים על ידי Network Monitor.
2. לכוד רק את כמות הנתונים הדרושים לך לשם הערכה. דבר זה ימנע ממך מללכוד כמויות גדולות של מידע ויאפשר לך אבחון קל ומהיר של הבעיה.

לאחר שיעור זה, תוכל

- ללכוד נתונים באמצעות Network Monitor.
- לבחון מסגרות באמצעות Network Monitor.
- לצפות בנתונים באמצעות Network Monitor.

זמן לימוד משוער: 40 דקות

בדיקת מסגרות

Network Monitor מסוגל ללכוד מסגרות הנשלחות אל ומאת מתאם הרשת. מסגרות (Frames) בנויות ממספר רב של פיסות מידע, וביניהן:

❖ הפרוטוקול בו נעשה שימוש

❖ כתובת המקור של המחשב ששלח את ההודעה

❖ כתובת היעד של המסגרת

❖ אורך המסגרת

➢ **כדי ללכוד מסגרות רשת**

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools ובחר Network Monitor.

   אם אתה מתבקש לבחור רשת ברירת מחדל ממנה יש ללכוד מסגרות, בחר ברשת המקומית ממנה אתה מעוניין ללכוד מסגרות כברירת מחדל.

2. פתח את תפריט Capture, ובחר Start.

צפייה בנתונים

לאחר שלכדת נתונים, תוכל לצפות בהם באמצעות ממשק Network Monitor, כפי שמוצג בתרשים 4.2. Network Monitor מבצע ניתוח חלקי באופן אוטומטי, מפני שהוא מתרגם נתונים גולמיים (Raw Data) שנלכדו ומארגן אותם למבנה של מסגרת לוגית. Network Monitor מציג גם סטטיסטיקה כוללת של מקטע הרשת, כולל:

❖ מסגרות Broadcast

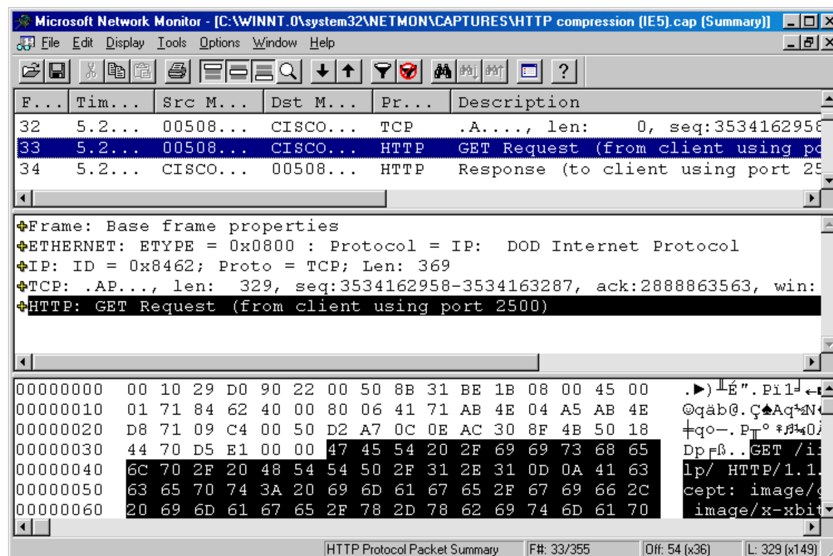
❖ מסגרות Multicast

❖ ניצולת רשת

❖ סך כל הבתים שהתקבלו בשנייה

❖ סך כל המסגרות שהתקבלו בשנייה

הערה מטעמי אבטחת מידע, Network Monitor של Windows 2000 לוכד את אותן מסגרות, כולל מסגרות Broadcast ומסגרות Multicast, שנשלחו אל ומאת המחשב המקומי.



תרשים 4.2 ממשק המשתמש של Network Monitor

Network Monitor מתפקד כמנהל התקן NDIS (**N**etwork **D**river **I**nterface) **S**pecification-Compliant) כדי להעתיק מסגרות לאוגר הלכידה, אזור אחסון בזיכרון אשר גודלו ניתן לשינוי. גודל ברירת המחדל הוא 1MB ; תוכל להתאים את גודלו באופן ידני, לפי הצורך. ודא כי קיים מספיק מקום פנוי בזיכרון, כדי לאפשר זאת.

הערה מאחר ו- Network Monitor משתמש במצב מקומי-בלבד (Local-Only) של NDIS, במקום במצב חסר האבחנה (בו עובר מתאם הרשת על כל המסגרות הנשלחות ברשת), אתה יכול להשתמש ב- Network Monitor גם אם מתאם הרשת שלך אינו תומך במצב חסר האבחנה (Promiscuous Mode). ביצועי הרישות אינם מושפעים כאשר אתה משתמש במנהל התקן NDIS ללכידת מסגרות (העבודה במצב חסר אבחנה עלולה להוסיף 30% **ויותר** עומס על המעבד).

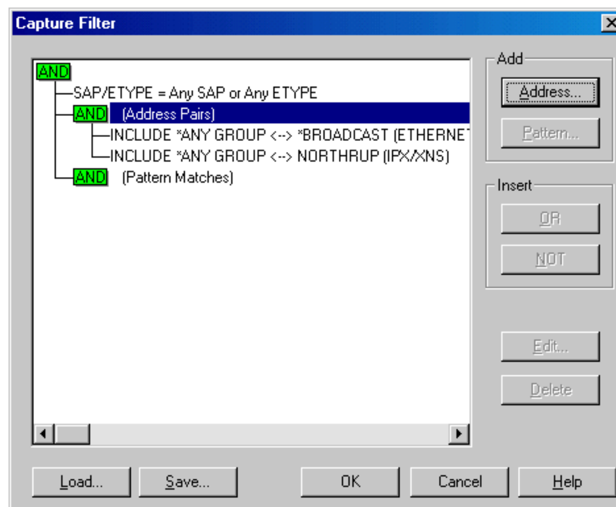
Network Monitor מציג סטטיסטיקת שיח (Session Statistics) מתוך 100 שיחי הרשת הייחודיים הראשונים שהוא מזהה. כדי לאפס את הסטטיסטיקות ולצפות במידע אודות

100 השיחים הבאים המזוהים, פתח את תפריט Capture ובחר Clear Statistics. חלון Capture של Network Monitor כולל את החלוניות הרשומות בטבלה 4.1.

טבלה 4.1 סטטיסטיקות המוצגות בחלון Capture

החלונית	מציגה
Graph	תצוגה גרפית של הפעילות המתרחשת ברגע זה ברשת
Session Stats	סטטיסטיקה לגבי שיחים בודדים המתרחשים כרגע ברשת
Station Stats	סטטיסטיקה לגבי השיחים בהם משתתף המחשב המפעיל את Network Monitor
Total Stats	סיכום סטטיסטי לגבי פעילות הרשת שזוהתה מאז החל תהליך הלכידה

כדי ללכוד רק את אותן מסגרות שמקורן במחשבים מסוימים, אתר את כתובותיהם של המחשבים ברשת שלך ושייך אותם למערכת DNS (**D**omain **N**ame **S**ystem) או שמות NetBIOS. לאחר שביצעת שיוכים אלה תוכל לשמור את השמות לקובץ מסד נתוני כתובות (בעל סיומת adr), אשר יוכל לשמש לעיצוב מסנני לכידה (Capture Filter) ומסנני תצוגה (Display Filter). מסנן לכידה מאפשר לך לציין קריטריון שייכלל או שלא ייכלל בלכידה. תרשים 4.3 מציג את תיבת דו-שיח Capture Filter, אליה ניתן לגשת מתפריט Capture, או על ידי הקשה על F8 בחלון Capture.



תרשים 4.3 תיבת דו-שיח Capture Filter

הערה מסנני לכידה יכולים להגדיל באופן משמעותי את העומס על המעבד (CPU), מפני שכל מנה חייבת להיות מעובדת דרך המסנן ואז או להישמר או שמתעלמים ממנה. במקרים מסוימים, השימוש במסננים מורכבים עלול לגרום למסגרות חסרות.

כדי לעצב מסנן לכידה, ציין הצהרות החלטה (Decision Statements) בתיבת דו-שיח Capture Filter.

על ידי ציון תבנית להתאמה במסנן הלכידה תוכל:

- להגביל את הלכידה למסגרות הנושאות סוג מסוים של נתונים.
- ללכוד מסגרות שנשלחו באמצעות פרוטוקול מסוים.
- להשתמש במזנק לכידה (Capture Trigger) להפעלת אירועים לאחר הלכידה.

טבלה 4.2 מתארת את סוגי המזנקים בהם תוכל להשתמש כדי לציין תנאי המפעיל מזנק.

טבלה 4.2 תיאור מזנקי לכידה

סוג המזנק	תיאור
Nothing	לא מופעל מזנק. זו ברירת המחדל.
Pattern Match	מפעיל את המזנק כאשר מזוהה תבנית מסוימת במסגרת הנלכדת.
Buffer Space	מפעיל את המזנק כאשר מתמלא נפח מוגדר של מאגר לכידה.
Pattern Match then Buffer Space	מפעיל את המזנק כאשר מזוהה תבנית מסוימת במסגרת הנלכדת, ולאחריה מתמלא אחוז מוגדר של נפח מאגר הלכידה.
Buffer Space then Pattern Match	מפעיל את המזנק כאשר מתמלא אחוז מוגדר של נפח מאגר הלכידה ולאחריו מזוהה תבנית מסוימת במסגרת הנלכדת.
No Action	לא מתבצעת פעולה כלשהי כאשר מתמלא תנאי להפעלת מזנק. זו ברירת המחדל. למרות שבחרת באפשרות No Action, המחשב יצפצף בכל פעם שמופיע תנאי להפעלת מזנק.
Stop Capture	מפסיק את פעולת הלכידה כאשר מתמלא תנאי להפעלת מזנק.
Execute Command Line	מפעיל תוכנית או קובץ אצווה כאשר מתמלא תנאי להפעלת מזנק. אם תבחר באפשרות זו ספק פקודה, או נתיב לתוכנית או לקובץ אצווה.

הערה אם במחשב שלך מותקנים מספר מתאמי רשת, החלף בין שני המתאמים או הפעל מספר מופעים של Network Monitor. כדי להחליף בין שני המתאמים, פתח את תפריט Capture, בחר Network ובחר מתאם.

לאחר לכידת הנתונים ייתכן שתרצה לשמור אותם. למשל, שמירת הנתונים היא פעולה יעילה לפני תחילתה של פעולת לכידה חדשה (כדי למנוע איבוד של נתוני הלכידה הקודמת) אם לדעתך יימצא הצורך לנתח את הנתונים בשלב אחר כלשהו, או אם עליך לתעד את תקלות הרשת שלך או את השימוש בה. כאשר אתה שומר את נתוני הלכידה, נרשמים הנתונים שבמאגר הלכידה (Capture Buffer) לקובץ בעל סיומת cap.

שימוש במסנני תצוגה

בדומה למסנן הלכידה, תוכל להיעזר גם במסנן תצוגה (Display Filter) כגון שאילתת מסד נתונים, כדי לציין איזה מסגרות להציג. מכיון שמסנן התצוגה פועל על נתונים שכבר נלכדו הוא אינו משפיע על תוכן מאגר הלכידה של Network Monitor.

ניתן לסנן מסגרת בהתבסס על הנתונים הבאים:

- כתובת היעד או המקור של שכבת קישור הנתונים או שכבת הרשת.
- הפרוטוקולים באמצעותם נשלחה המנה או המסגרת.
- המאפיינים והערכים שמכילה המסגרת (מאפיין, Property, הוא שדה נתונים בכותרת הפרוטוקול. כל מאפייני הפרוטוקול מציינים את מטרת הפרוטוקול).

כדי לעצב מסנן תצוגה, ציין הצהרות החלטות (Decision Statements) בתיבת דו-שיח Display Filter. מבנה המידע בתיבת דו-שיח Display Filter דומה לזה של עץ קבלת החלטות, שהוא ייצוג גרפי של לוגיקת המסנן. כאשר אתה משנה מפרטים של מסנני תצוגה, משקף עץ קבלת ההחלטות (Decision Tree) את השינויים הללו. טבלה 4.3 מציגה סוגים שונים של פריטי מסנן בהם תוכל להשתמש.

טבלה 4.3 סוגי מסנני תצוגה

פריט המסנן	תיאור
Protocol	**מציין את מאפייני הפרוטוקול או הפרוטוקולים.**
Address Filter (ברירת המחדל היא ANY <--> ANY)	**מציין את כתובות המחשב בו אתה מעוניין ללכוד את הנתונים.**
Property	**מציין את מופעי מאפיינים התואמים לקריטריוני התצוגה שלך.**

במסנני התצוגה תוכל להשתמש בלוגיקת AND, OR ו-NOT, ושלא כמו במסנני לכידה תוכל להשתמש ביותר מאשר ארבעה ביטויי מסנן כתובת (Address Filter). כאשר אתה מציג נתונים שנלכדו, כל המידע הזמין אודות הנתונים הלכודים מופיע בחלון Frame Viewer. כדי להציג רק את אותן מסגרות שנשלחו באמצעות פרוטוקול מסוים, ערוך את השורה Protocol בתיבת דו-שיח Display Filter. מאפייני פרוטוקול הם נתונים הנגזרים ממידע הכלול בנתוני הפרוטוקול. מכיון שלכל פרוטוקול יש מטרה שונה, משתנים בהתאם גם מאפייניהם של הפרוטוקולים השונים. נניח לדוגמה, שלכדת כמות גדולה של מסגרות באמצעות פרוטוקול SMB (**S**erver **M**essage **B**lock), וכעת אתה מעוניין לבחון רק את אותן מסגרות בהן נעשה שימוש ב-SMB כדי ליצור ספריה במחשב שלך. במקרה כגון זה, תוכל לבחון רק מסגרות בהן המאפיין command של SMB שווה ל- make directory. יתר על כן, תוכל להציג רק מסגרות שמקורן במחשב מסוים, על ידי עריכת השורה ANY <--> ANY שבתיבת דו-שיח Display Filter.

סקירת נתונים שנלכדו

פעל על פי הצעדים שברשימה הבאה כחלק משגרת הסקירה וניתוח הנתונים שלכדת:

- עקוב אחר שיח (Session) תוך שימוש בכתובות IP של יעד ומקור ומספרי יציאות (Port).
- אם איתרת Reset, התמקד במספרים הרציפים ובאישורי הקבלה הקודמים להם.

❖ היעזר במחשבון כדי לראות איזה אישורי קבלה משויכים לנתונים שנשלחו.

❖ נסה להבין את הפעילות בה אתה צופה:

✱ האם השולח מבצע שידורים חוזרים?

✱ אם כן, שים לב למספר השידורים החוזרים ולמשך הזמן ביניהם. מספר ברירת המחדל לשידורים חוזרים המוגדר לפרוטוקול TCP/IP הוא 5. ייתכן שבפרוטוקולים אחרים המספר שונה.

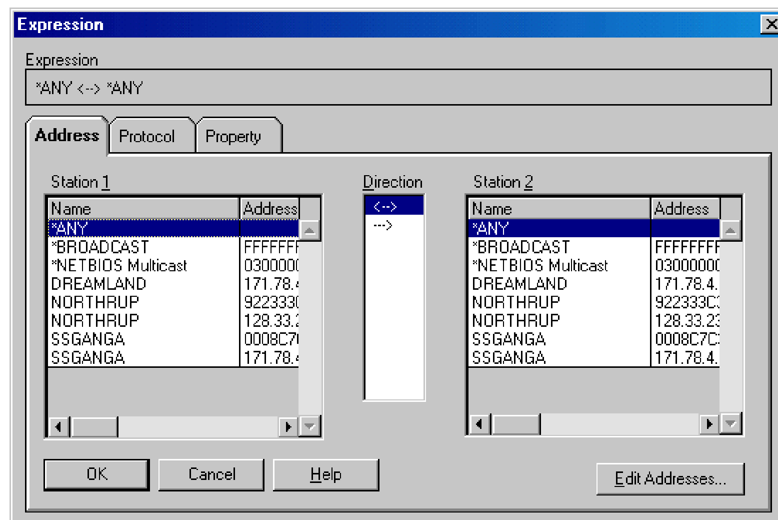
✱ האם השולח נסוג ושלח מנה קודמת?

✱ האם המקבל מבקש מסגרת חסרה על ידי מתן אישור למספר סודר קודם?

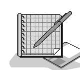
איפוס (Reset) יכול להיגרם על ידי פסקי-זמן (Time-outs) בשכבת TCP, או על ידי פסקי-זמן בפרוטוקולים עיליים (Higher-Level Protocols). איפוסים המתרחשים בשכבת TCP צריכים להיות קלים לקריאה מהמעקב. ייתכן שיהיה זה קשה יותר לקבוע את המקור לאיפוסים המתרחשים בפרוטוקולים עיליים, כגון SMB.

לדוגמה, קריאת SMB עשויה לקבל פסק-זמן לאחר 45 שניות, מה שיגרום לאיפוס השיח (Session), למרות שהתקשורת איטית, אבל קיימת, בשכבת TCP. רשומת המעקב (Trace) עשויה רק לצמצם את האפשרויות לאיזה רכיב גורם לתקלה. מנקודה זו ואילך ייתכן שתצטרך להשתמש בשיטות אחרות לאיתור תקלות כדי לקבוע את הסיבה.

כדי לראות סידורי TCP (TCP Sequencing) כאשר נוכחים פרוטוקולים עיליים, הפעל את Network Monitor וערוך את תיבת דו-שיח Expression, תוך שימוש בצעדים המתוארים בתרגול הבא. תרשים 4.4 מציג את תיבת דו-שיח Expression.



תרשים 4.4 תיבת דו-שיח Expression



תרגול: לכידת מסגרות באמצעות Network Monitor

תוכל להיעזר ב- Network Monitor ללכידת מסגרות משטף הנתונים, ולהעתיק מסגרות אלו לקובץ לכידה זמני. בתרגול זה תשתמש ב- Network Monitor כדי להציג סטטיסטיקות לגבי מסגרות הנלכדות באופן דינמי בחלון Capture, ותעצב מסנן לכידה כך שיעתיק רק את המסגרות התואמות לקריטריון מסוים שתציב.

➢ **כדי לראות סידרור TCP**

1. הפעל את Network Monitor.
2. הצג נתונים שנלכדו.
3. פתח את תפריט Display, ובחר Options.
4. בחר Auto (בהתאם לפרוטוקולים שבמסנן התצוגה), ולחץ OK.
5. פתח את תפריט Display, ובחר Filter.
6. לחץ לחיצה כפולה על Protocol=Any.
7. בחר בכרטיסיה Protocol, ולחץ על Disable All.
8. בתיבת הרשימה Disabled Protocols סמן TCP.
9. לחץ Enable, ולחץ OK.
10. פתח את תפריט Capture, ובחר Start.

ביצועי Network Monitor

Network Monitor יוצר קובץ ממופה זיכרון עבור מאגר הלכידה שלו. לשם קבלת התוצאות הטובות ביותר ודא שאתה יוצר מאגר לכידה הגדול דיו לאחסון כל התעבורה הדרושה לך. בנוסף, למרות שאינך יכול להתאים את גודל המסגרות, תוכל לאחסן רק חלק ממנה. בדרך זו את מקטין את הנפח המבוזבז לריק של מאגר הלכידה. לדוגמה, אם אתה מעוניין רק בנתונים שבכותרת המסגרת, קבע את גודל המסגרת (בבתים, Bytes) לזה של כותרת המסגרת. כאשר הנתונים הנלכדים יאוחסנו למאגר הלכידה, ייפטר Network Monitor מהנתונים במסגרת, ובכך יקטין את נפח הנתונים הנאגרים.

זיהוי Network Monitor

כדי להגן על הרשת שלך מפני שימוש לא מורשה בהתקנות של Network Monitor, יכול Network Monitor לזהות התקנות אחרות של Network Monitor הפועלות במקטע הרשת המקומי. כאשר Network Monitor מזהה התקנות אחרות של Network Monitor הפועלות ברשת הוא מציג את המידע הבא:

❖ שם המחשב
❖ שם המשתמש המחובר במחשב זה

- מצב Network Monitor במחשב המרוחק (פעיל, לוכד או משדר)
- כתובת מתאם הרשת של המחשב המרוחק
- מספר הגירסה של Network Monitor הפועל במחשב המרוחק

במקרים מסוימים, ארכיטקטורת הרשת שלך עשויה למנוע מהתקנה אחת של Network Monitor לזהות התקנה אחרת. לדוגמה, אם התקנה כלשהי מופרדת משלך באמצעות נתב שאינו מעביר שידור מרובה (Multicast), ההתקנה שלך לא תצליח לזהות התקנה זו.

סיכום שיעור

Network Monitor מנטר את שטף הנתונים ברשת, אשר כולל את כל המידע המועבר ברשת בכל רגע נתון. תוכל להיעזר במסנן תצוגה כדי לקבוע איזה מסגרות להציג. כדי לעצב מסנן לכידה עליך לציין הצהרות החלטות (Decision Statements) בתיבת דו-שיח Capture Filter. לאחר שלכדת נתונים, תוכל לצפות בהם באמצעות ממשק המשתמש של Network Monitor. ודא כי אתה מגדיר מאגר לכידה גדול דיו לאחסון כל התעבורה הדרושה לך.

שיעור 3: כלי ניהול ב- Windows 2000

למערכת ההפעלה Windows 2000 יש כלים וטכנולוגיות שנועדו להקל עליך את משימות הניהול של מחשבים ברשת שלך. Terminal Services מספקים למחשבי לקוח גישה ל- Windows 2000 וליישומים מבוססי-Windows העדכניים ביותר. הם גם מאפשרים למנהלי מערכות (System Administrators) לנהל מרחוק משאבי רשת. יתר על כן, יחד עם Windows 2000 תמצא את **S**imple **N**etwork **M**anagement **P**rotocol (SNMP), המאפשר לך לנטר ולתקשר מידע מצב מסוכני SNMP (SNMP Agents) לבין תוכנות ניהול לרשת. בשיעור זה תלמד כיצד להשתמש ב- Terminal Services וב-SNMP כדי לנהל טוב יותר ולנטר את הרשת שלך.

לאחר שיעור זה, תוכל

- להגדיר Terminal Server לניהול מרחוק.
- להתקין ולהגדיר את שירות SNMP.
- לתאר כיצד פועל שירות SNMP בסביבת Windows 2000.

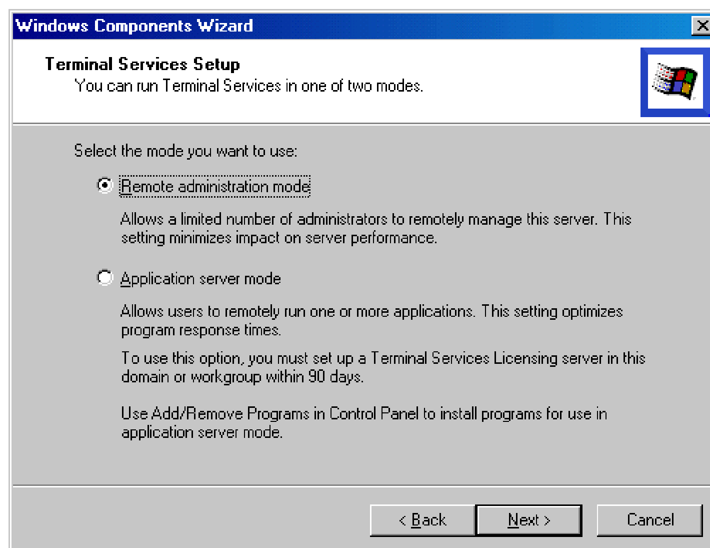
זמן לימוד משוער: 25 דקות

אפשרויות הניהול של Windows 2000

באמצעות Windows 2000 תוכל לנהל מחשבים ושירותים ברשת שלך באופן מקומי, או מרחוק. לניהול מרחוק (Remote Administration) נחשב השימוש במחשב אחד לצורך התחברות למחשב אחר ברשת, למטרות ניהול. Windows 2000 מאפשרת לך לבצע משימות ניהול מרחוק בכל המחשבים ברשת באופן מרוכז, במקום במיקומו הפיסי של כל מחשב ומחשב. תוכל להשתמש במערכת ניהול של צד-שלישי, או להשתמש בחלק מהכלים והשיטות שמספקת Windows 2000 לצורך זה.

Terminal Services

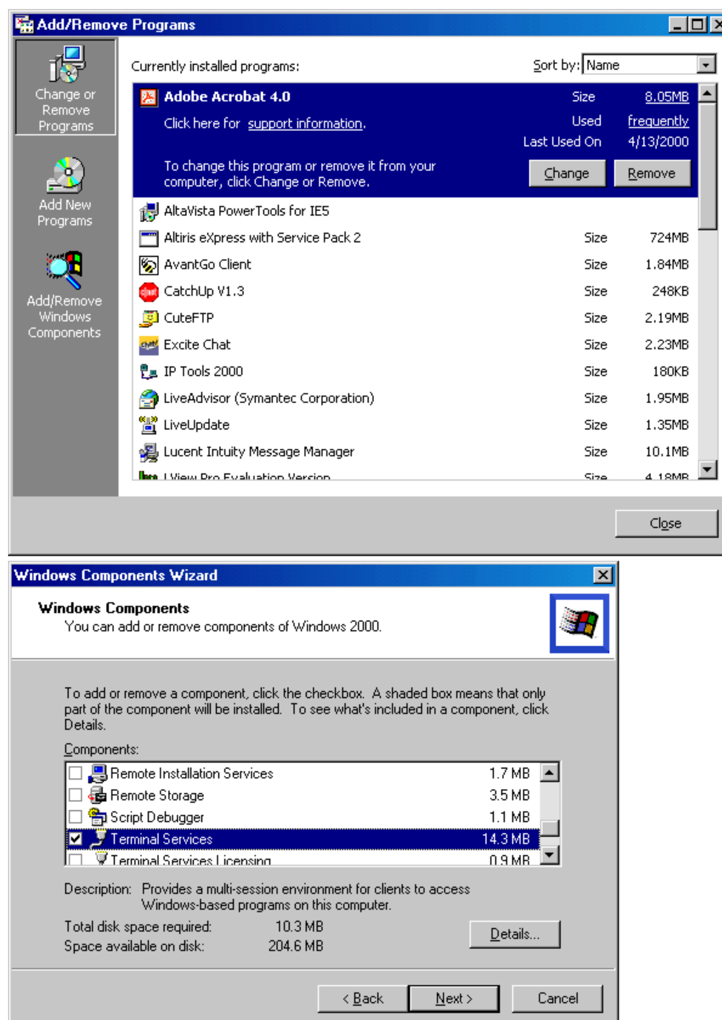
כאשר אתה מאפשר את Terminal Services במחשב Windows 2000 Server אתה בוחר בין שני מצבים אפשריים: Remote Administration או Application Server. ראה תרשים 4.5.



תרשים 4.5 בחירת מצב עבור Terminal Services

מצב Application Server (שרת יישומים) מאפשר לך להטמיע ולנהל יישומים ממיקום מרכזי אחד. תוכל להטמיע גם את ממשק Windows 2000, בנוסף ליישומים, למחשבים שאינם מסוגלים להפעיל את מערכת ההפעלה הזו. מכיון ש- Terminal Services הם חלק אינטגרלי מהמוצר Windows 2000 Server, תוכל להפעיל את היישומים שלך בשרת ולספק את ממשק המשתמש ללקוחות שאינם מסוגלים להפעיל Windows 2000, כגון מחשבים הפועלים בסביבת Windows 3.11 או בסביבת Windows CE, המחוברים ל- Terminal Server.

Terminal Services מציעים גם מצב ניהול מרחוק המאפשר לך לגשת, לנהל ולאתר תקלות בלקוחות. מצב ניהול מרחוק (Remote Administration) מאפשר לך לנהל מרחוק שרתי Windows 2000 בכל חיבור TCP/IP, כולל גישה מרחוק, Ethernet, האינטרנט, חיבור אלחוטי, רשתות רחבות (WAN) או רשתות וירטואליות פרטיות (VPN). ניתן להתקין את Terminal Services מתיבת דו-שיח Windows Components שביישומון לוח הבקרה Add/Remove Programs, כפי שמתואר בתרשים 4.6.



תרשים 4.6 אפשרות התקנת Terminal Services

שימוש ב- Terminal Server

למרות שבעת התקנת Terminal Services מוגדר באופן אוטומטי פרוטוקול RDP (**R**emote **D**esktop **P**rotocol), תוכל להיעזר בצעדים הכלליים הבאים כדי ליצור חיבור חדש. לכל מתאם רשת ב- Terminal Server ניתן להגדיר רק RDP אחד; אבל, תוכל להגדיר חיבורי RDP נוספים אם תתקין מתאם רשת עבור כל חיבור במחשב שלך.

➢ כדי להתקין מתאם רשת

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ובחר Terminal Services Configuration.
2. לחץ לחיצה ימנית על הכרטיסיה Connections, ובחר Create New Connection.

   מופיע Terminal Services Connection Wizard.
3. בתיבת דו-שיח הראשונה של האשף עליך לבחור את סוג החיבור, למשל Microsoft RDP 5.0.
4. בתיבת דו-שיח השנייה של האשף עליך לקבוע את רמת ההצפנה (Low, Medium או High). תוכל גם לבחור באפשרות Standard Windows Authentication.
5. בתיבת דו-שיח השלישית של האשף תוכל לקבוע אפשרויות שליטה מרחוק ואת רמת השליטה.
6. בתיבת דו-שיח הרביעית באשף עליך לבחור בשם החיבור, סוג התעבורה והערה (אופציונלי).
7. בתיבת דו-שיח החמישית באשף תוכל לבחור באחד או בכל מתאמי הרשת עבור סוג התעבורה, ולקבוע את מספר החיבורים.
8. לחץ Finish כדי לסגור את האשף.

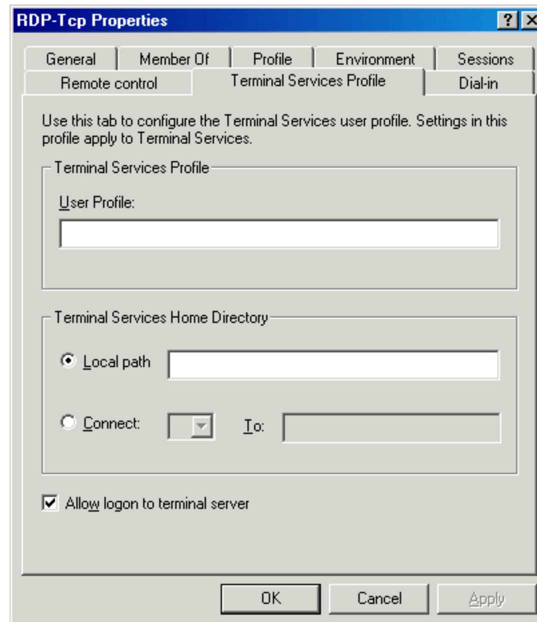
Terminal Services מאפשר עד שני חיבורי Remote Administration בו-זמנית, מבלי לדרוש רישיון. ללקוח Terminal Services נדרשים כמות זניחה של נפח דיסק פנוי, זיכרון והגדרות.

➢ כדי לאפשר למחשב לקוח של Terminal Server להתחבר ל- Terminal Server של Windows 2000

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ובחר Computer Management.
2. כדי לפרוש את ענפי התצוגה, לחץ על הסימן + שליד System Tools, לחץ על הסימן + ליד Local Users and Groups ולחץ על הסימן + ליד Users.
3. לחץ לחיצה כפולה על רשומת המשתמש לו אתה מעוניין לאפשר להתחבר כלקוח Windows NT Terminal Server.
4. בכרטיסיה Terminal Services Profile, סמן את תיבת הסימון Allow logon to terminal server, כפי שמוצג בתרשים 4.7.
5. סגור את תיבת דו-שיח Computer Management.
6. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ולחץ על Terminal Services Configuration.
7. פתח את התיקיה Connections.
8. פתח את תפריט Action ובחר Properties.
9. בכרטיסיה Permissions, הוסף את המשתמשים ו/או הקבוצות להם אתה מעוניין שתתאפשר גישה ל- Windows NT Terminal Server זה.

10. לחץ OK כדי לסגור את תיבת דו-שיח Properties של החיבור.

11. סגור את Terminal Services Configuration.



תרשים 4.7 אפשור כניסה לשרת המסוף

SNMP

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) הוא פרוטוקול ניהול לרשת בו נעשה שימוש נרחב ברשתות מבוססות TCP/IP, כדי לנטר ולנהל מחשבים והתקנים אחרים (כגון מדפסות) המחוברים לרשת. את SNMP ניתן להתקין בכל מחשב הפועל בסביבת Windows 2000 ועם הפרוטוקולים TCP/IP או IPX/SPX.

➢ כדי להתקין את שירות SNMP

1. לחץ Start, הצבע על Settings, ובחר את Control Panel. לחץ לחיצה כפולה על Add/Remove Programs, ולחץ על Add/Remove Windows Components.

   מופיע חלון Windows Component Wizard.

2. בתיבה Components לחץ על Management and Monitoring tools, ולחץ Details.

   מופיעה תיבת דו-שיח Management and Monitoring tools.

3. סמן את תיבת הסימון Simple Network Management Protocol, ולחץ OK.

4. בחלון Windows Component Wizard לחץ Next.

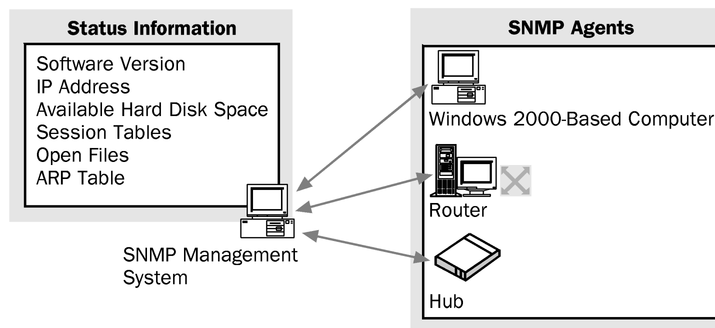
   האשף Windows Component מתקין את SNMP.

5. לחץ Finish כדי לסגור את Windows Component Wizard.

מערכות ניהול וסוכנים

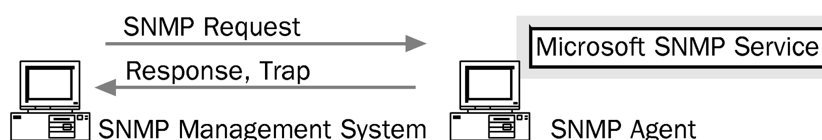
SNMP כולל מערכות ניהול (Management Systems) וסוכנים (Agents). מערכת ניהול היא כל מחשב בו פועלת תוכנת הניהול של SNMP. למרות ש- Windows 2000 אינה כוללת מערכת ניהול, קיימים כלים רבים של צד-שלילי הזמינים לסביבת עבודה זו. ביניהם ניתן למצוא את Net Manager של חברת Sun או את Open View של חברת HP. מערכת ניהול מבקשת מידע מהסוכן.

כפי שהדבר מתואר בתרשים 4.8, סוכן (Agent) הוא כל מחשב בו פועל סוכן SNMP (SNMP Agent), כגון מחשב מבוסס-Windows 2000, נתב או רכזת (Hub). שירות SNMP של Microsoft הוא תוכנת סוכן SNMP. הפעילות העיקרית של סוכן היא לבצע פעולות אותן מבקשת מערכת הניהול.



תרשים 4.8 סוכני SNMP

רכיב הסוכן של SNMP מאפשר למחשב Windows 2000 להיות מנוהל מרחוק. הפעולה היחידה המופעלת על ידי הסוכן נקראת Trap (מלכודת). Trap היא הודעה הנשלחת על ידי הסוכן למערכת הניהול ומציינת שהתרחש אירוע במארח המפעיל את הסוכן. כפי שניתן לראות בתרשים 4.9, יישום תוכנת הניהול של SNMP לא חייב לפעול באותו מחשב בו פועל סוכן SNMP.



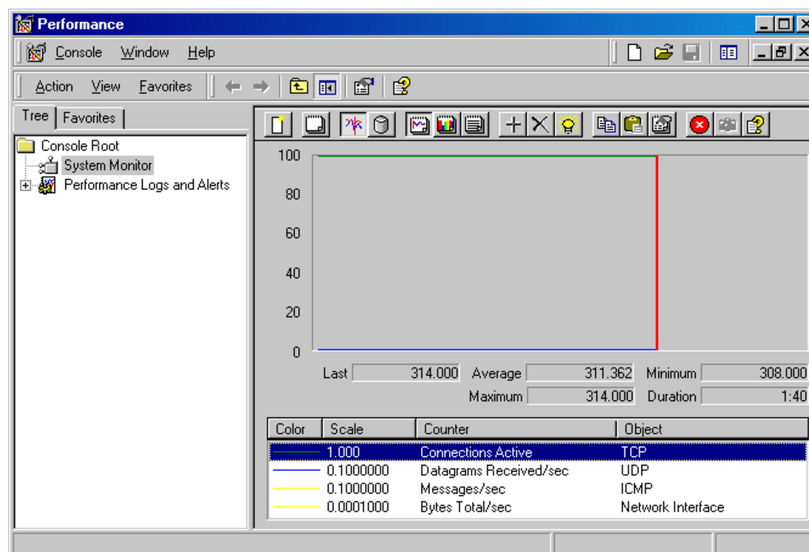
תרשים 4.9 מערכת ניהול SNMP והסוכן

יתרונות SNMP

אם התקנת את שרת DHCP, IIS או תוכנת שרת WINS במחשב מבוסס Windows 2000 ברשת, תוכל לנטר שירותים אלה תוך שימוש בתוכנת מנהל SNMP. יתר על כן, תוכל להשתמש ב- Performance Monitor כדי לבחון מוני ביצועים הקשורים ל- TCP/IP. כאשר אתה מתקין את שירות SNMP, הופכים מוני הביצועים של TCP/IP לזמינים

ב- Performance Monitor. אובייקטי TCP/IP הנוספים כוללים את: ICMP, TCP, IP, UDP, DHCP, WINS, FTP, ממשק רשת (Network Interface) ו- IIS (**I**nternet **I**nformation **S**erver).
כפי שניתן לראות בתרשים 4.10, Performance Monitor יכול למנות:

- ❖ חיבורי TCP פעילים
- ❖ מספר צרורות UDP המתקבלים בשנייה
- ❖ מספר הודעות ICMP המתקבלות בשנייה
- ❖ סך כל בתי הממשק המתקבלים בשנייה



תרשים 4.10 מוני Performance Monitor הנוספים

סיכום

SNMP הוא פרוטוקול ניהול רשת בו נעשה שימוש נרחב ברשתות מבוססות TCP/IP. הוא יכול לתקשר בין תוכנת ניהול המופעלת על ידי מנהל רשת לבין סוכן ניהול רשת המופעל ב-Host או ב-Gateway. תוכל להשתמש ב-SNMP גם כדי לנטר ולשלוט מרחוק במארחים ובשערים באגד רשתות (Internetwork). שירות SNMP של Windows 2000 מאפשר למחשב מבוסס-Windows 2000 להיות מנוטר ומנוהל מרחוק. שירות SNMP יכול לטפל בבקשות ממארח אחד או יותר, ויכול גם לדווח נתוני מערכת ניהול למארח אחד או יותר בבלוקים חסויים של מידע, הנקראים מלכודות (Traps). כאשר אתה מתקין את SNMP, הופכים מספר מוני ביצועים של TCP/IP לזמינים בשירות Performance Monitor.

שאלות סיכום

השאלות הבאות נועדו לחזק את הנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות על שאלה, עיין בשיעור המתאים ונסה את השאלה שנית. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואחר כך בעברית.

Answering the following questions will reinforce key information presented in this chapter. If you are unable to answer a question, review the appropriate lesson and then try the question again. Answers to the questions can be found in Appendix A, "Questions and Answers".

1. What is the purpose of analyzing frames with Network Monitor?
2. What kind of data does a frame contain?
3. What is a capture filter, and what is it used for?

1. לשם מה יש לנתח מסגרות באמצעות Network Monitor?
2. איזה סוג נתונים מכילה המסגרת?
3. מהו מסנן לכידה, ולמה הוא משמש?

פרק 5

יישום IPSec

אודות פרק זה

כדי לשמור על חסיונו של המידע ברשת תוכל להשתמש בפרוטוקול אינטרנט מאובטח (IPSec, **I**nternet **P**rotocol **Sec**urity), כדי להצפין את תעבורת הרשת בין חלק או כל המחשבים ברשת שלך. IPSec מאפשר לך להגדיר חיבורים מאומתים ומוצפנים בין שני מחשבים. בפרק זה תלמד כיצד לאפשר, להגדיר ולנטר את IPSec. בנוסף תלמד גם כיצד להתאים את מדיניות וכללי IPSec התאמה אישית.

לפני שתתחיל

להשלמת פרק זה צריך שיהיה לך:

❖ שני מחשבים בהם מותקן שרת Windows 2000, ובשניהם גם מותקן Network Monitor גירסה 2.0.

שיעור 1: סקירה ואפשור IPSec

מזה זמן מהווה IPSec נקודת הכיוון לאבטחת רישות. הוא מספק קו עיקרי של אבטחה מפני התקפות על רשתות קטנות כגדולות, פרטיות והאינטרנט כאחד, תוך שהוא מאזן בין הקלות בשימוש לבין אבטחת מידע. שיעור זה דן באוסף הטכנולוגיות, הנקראות בשם הכולל IPSec (**I**nternet **P**rotocol **Sec**urity).

לאחר שיעור זה, תוכל

- להסביר את יתרונותיו של IPSec.
- לתאר את ארכיטקטורת IPSec.

זמן לימוד משוער: 50 דקות

Internet Protocol Security

עם התפתחותה של רשת האינטרנט, ולצידה רשתות האינטראנט, גדל גם הצורך באבטחת הנתונים. התחומים העיקריים מפניהם יש להגן הם:

- שינוי הנתונים בעודם עוברים ברשת.
- לכידה, צפייה או העתקה בעת לכידה.
- גישה לא מורשית לרשת.

IPSec היא סביבת עבודה של תקנים פתוחים להבטחת תקשורת פרטית מאובטחת ברשתות מבוססות-IP, באמצעות השימוש בשירותי אבטחה וקריפטוגרפיה (הצפנה). יישום IPSec בסביבת Windows 2000 מבוסס על על התקנים שפותחו על ידי קבוצת העבודה של IPSec בכוח המשימה ההנדסי של האינטרנט, IETF (**I**nternet **E**ngineering **T**ask **F**orce). ל- IPSec יש שתי מטרות:

1. להגן על מנות IP.
2. לספק הגנה מפני התקפות על הרשת.

שתי מטרות אלו הושגו תוך שימוש בשירותי הגנה מבוססי-הצפנה, פרוטוקולי אבטחה וניהול דינמי של מפתחות. יסוד זה מספק את העוצמה ואת הגמישות המאפשרים להגן על התקשורת בין מחשבים ברשת פרטית ומחשבים מרוחקים המחוברים באמצעות האינטרנט, לבין לקוחות חיוג (Dial-up). ניתן אף להשתמש בו כדי לסנן מנות נתונים ברשת.

IPSec מבוסס על מודל האבטחה קצה-לקצה (End-to-End Security Model), מה שאומר שהמחשבים היחידים שחייבים לדעת אודות IPSec הם המחשבים השולחים והמקבלים. כל אחד מאלה מטפל בנושא האבטחה בצד הנוגע לו, תוך שהוא יוצא מנקודת הנחה שהמדיום באמצעותו מבוצעת ההתקשרות אינו מאובטח. נתבים המעבירים מנות בין מקורות ויעדים אינם נדרשים לתמוך ב-IPSec.

מודל זה מאפשר ל-IPSec להיות מיושם בהצלחה ברשתות קיימות, כגון:

❖ רשת מקומית (LAN): שרת/לקוח, Peer-to-Peer

❖ רשת מרחבית (WAN): נתב לנתב

❖ גישה מרחוק: לקוחות בחיוג וגישה מהאינטרנט מרשתות פרטיות

הגנה לעומק

יש להגן על נתונים מפני לכידה, שינוי או גישה על ידי צדדים שאינם מורשים בכך. התקפה על רשת יכולה לגרום להפסקת פעולה (Downtime) או לחשיפה ציבורית של מידע רגיש.

אסטרטגיות הגנה על רשת מתמקדות בדרך כלל רק במניעת התקפות מחוץ לרשת הפרטית על ידי שימוש בחומות אש (Firewall), נתבים מאובטחים (שערי אבטחה) ואימות משתמשים למשתמשי גישה בחיוג. דבר זה נקרא אבטחה היקפית, ואינו מגן מפני התקפות מתוך הרשת.

שיטות לאבטחה ברמת גישת-משתמשים (כגון כרטיסים חכמים או אימות Kerberos גירסה 5) אינן מתאימות להגנה מפני רוב ההתקפות ברמת-הרשת, מפני שהן מסתמכות רק על שם המשתמש וסיסמתו. מחשבים רבים משותפים למשתמשים רבים. כתוצאה מכך, נשאר המחשב פעמים רבות במצב Logged-on (לא התבצעה יציאה מסודרת של המשתמש מהמערכת) ובכך הוא הופך ללא מאובטח. אם נחשפו שמו וסיסמתו של משתמש, לא תצליח האבטחה ברמת גישת-משתמש למנוע מהמתקיף לגשת למשאבי הרשת.

אסטרטגיות הגנה ברמה הפיסית מגינות על חיווט הרשת מפני גישה, ועל נקודות הגישה מפני שימוש. אבל, אסטרטגיות אלו אינן יכולות להבטיח הגנה כאשר המידע עובר דרך מספר רשתות, כפי שמתחייב מהעבודה ברשת האינטרנט. במקום זאת, השיטה הטובה ביותר להגנה על מידע מסופקת על ידי IPSec ומודל קצה-לקצה (End-to-End) שלו: המחשב השולח מצפין את הנתונים קודם לשידורם (עוד קודם להגעתם לחיווט הרשת) ואילו המחשב המקבל מפענח את הנתונים רק לאחר שקיבל את כולם. מסיבה זו צריך IPSec להיות אחד מהמרכיבים העיקריים בתכנון תשתית האבטחה הכללית בארגון, הוא מגן על המידע הפרטי שלך בסביבה ציבורית על ידי אספקת הגנה חזקה מבוססת-הצפנה כנגד התקפות. תוך שילוב עם בקרה ברמת-משתמש ואבטחה היקפית וברמה הפיסית, מבטיח IPSec הגנה מעמיקה לנתוניך.

יתרונות IPSec

IPSec של Windows 2000 מיושם באופן שקוף למשתמש. משתמשים אינם חייבים להיות חברים באותו Domain כדי לתקשר באמצעות אבטחת IPSec. הם יכולים להיות בכל אחד מה-Trusted Domains בארגון. ניהול IPSec מאפשר ריכוז הניהול. מדיניות אבטחה נוצרות על ידי Domain Administrator עבור רוב תרחישי ההתקשרות השכיחים. מדיניות אלו מאוחסנות ב- Directory Services ומשויכות ל- Domain Policies.

בכל פעם שמחשב מתחבר ל-Domain הוא מוריד באופן אוטומטי את מדיניות האבטחה שלו, תוך המנעות מהצורך להגדיר כל מחשב בנפרד. IPSec של Windows 2000 מספק את היתרונות הבאים כדי להשיג רמה גבוהה של תקשורת מאובטחת בעלות נמוכה:

- ניהול מרוכז של מדיניות אבטחה, מה שמפחית את עלויות הניהול.
- שקיפות IPSec בפני המשתמשים והיישומים.
- גמישות בהגדרת מדיניות אבטחה העונה על צרכים משתנים בארגון.
- שירותי חיסיון, המונעים גישה שאינה מורשית לנתונים רגישים, בעוד ש-IPSec עובר בין הצדדים המתקשרים.
- שירותי אימות חזקים המוודאים את זהותם של השולח והמקבל, כדי למנוע פגיעות באבטחה, הנובעות משימוש בזהויות שאולות.
- כל מנה מוצפנת תוך שימוש במידע מוכוון-שעון, כדי למנוע ממידע מלהילכד ולהישלח ליעדו המקורי במועד מאוחר יותר (ולכן חשוב ביותר להגדיר כהלכה את אזור הזמן ואת שעון המערכת!).
- מפתחות ארוכים במיוחד ומיפתוח דינמי מחדש, תוך כדי ההתקשרות, מסייע לשמירה מפני התקפות.
- קישורים מאובטחים מקצה-לקצה למשתמשי רשתות פרטיות בתוך אותו Domain או בין Trusted Domains בארגון.
- קישורים מאובטחים מקצה-לקצה בהתבסס על כתובות IP, בין משתמשים מרוחקים למשתמשים ב-Domain כלשהו בארגון.

יישום פשוט

כדי להשיג תקשורת מאובטחת בעלות נמוכה, מפשטת Windows 2000 את תהליך היישום של IPSec על ידי התכונות הבאות:

שילוב במסגרת האבטחה של Windows 2000

IPSec משתמש ב- Windows 2000 Secure Domain כ- Trust Model שלו. מדיניות ברירת המחדל של IPSec משתמשת בשיטת אימות ברירת המחדל של Windows 2000 (אימות Kerberos גירסה 5) כדי לזהות ולסמוך על מחשבים מתקשרים. מחשבים החברים ב- Windows 2000 Domain או ב- Trusted Domain יכולים ליצור התקשרות IPSec ללא קושי.

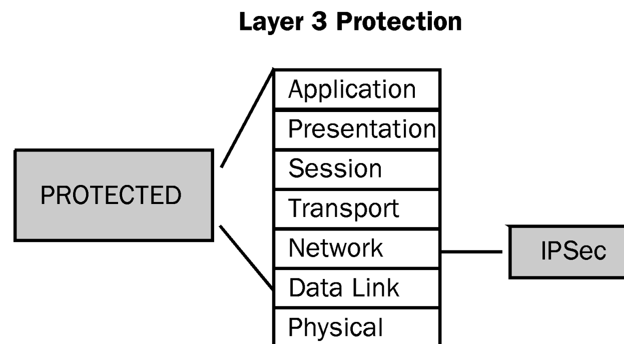
מרכוז ניהול מדיניות IPSec ברמת Active Directory

ניתן לשייך מדיניות IPSec באמצעות תכונת המדיניות הקבוצתית (Group Policy) של Active Directory. הדבר מאפשר למדיניות IPSec להיות משויכת ברמת היחידה הארגונית או ברמת ה- Domain, מה שיפחית את עומס הניהול הנדרש לשם הגדרת כל מחשב באופן פרטני.

שקיפות IPSec בפני משתמשים ויישומים

רמת האבטחה הגבוהה של IPSec היא תוצאה של יישומו ברמת תעבורת ה-IP (שכבה 3 של הרשת). יישום האבטחה ברמה 3 (ראה תרשים 5.1) מספק אבטחה לפרוטוקולים ברמה

עליונה יותר שבפרוטוקולים TCP/IP, כגון TCP, UDP, HTTP ואפילו פרוטוקולים מותאמים השולחים תעבורה בשכבת ה-IP. היתרון העיקרי של אבטחת מידע ברמה נמוכה זו טמון בכך שכל היישומים והשירותים המשתמשים ב-IP להעברת הנתונים שלהם, יכולים להיות מאובטחים באמצעות IPSec. זהו שיפור של מנגנוני אבטחה קודמים הפועלים מעל שכבה 3, כגון SSL (**S**ecure **S**ocket **L**ayer), אשר מגינים רק על יישומים המשתמשים ב-SSL. אם נדרשת אבטחה לכל היישומים, תידרש לשם כך התאמתם של כל היישומים .



תרשים 5.1 הגנת שכבה 3

גמישות בהגדרת אבטחה

ניתן להתאים באופן אישי את כל שירותי האבטחה בכל מדיניות, כדי לקיים את מרבית דרישות האבטחה לתעבורת הנתונים ברשת.

ניהול מפתחות אוטומטי

שירותי IPSec מחליפים ומנהלים באופן דינמי מפתחות הצפנה בין המחשבים המתקשרים.

מו"מ אבטחה אוטומטי

שירותי IPSec מנהלי באופן דינמי משא ומתן לגבי ערכת דרישות אבטחה אחידה בין המחשבים המתקשרים, ובכך מפחיתים את הצורך במדיניות זהה בשני המחשבים.

תמיכה בתשתית המפתח הציבורי

קיימת תמיכה בשימוש באישורי מפתח ציבורי לשם אימות, כדי לאפשר אימות ותקשורת מאובטחת עם מחשבים שאינם שייכים ל- Windows 2000 trusted domain.

תמיכה בקדם-שיתוף מפתח

אם לא מתאפשר אימות מבוסס kerberos גירסה 5 או מבוסס אישור מפתח ציבורי, ניתן להגדיר מפתח קדם-שיתוף (Preshare Key, סיסמה סודית משותפת), כדי לאפשר אימות וסמיכות בין מחשבים מתקשרים.

תהליך האבטחה של IP

לפניך סקירה קצרה לגבי תהליך האבטחה של IP, כפי שמתוארת בתרשים 5.2 :

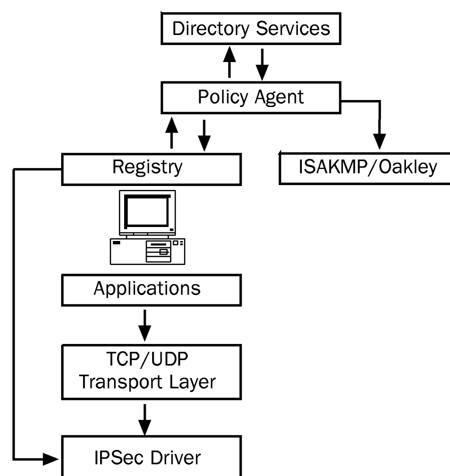
❖ מנת IP תואמת למסנן IP שהוא חלק ממדיניות IPSec.

❖ למדיניות IPSec יכולות להיות מספר שיטות אבטחה אופציונליות. מנהל ההתקן של IPSec צריך לדעת באיזו שיטה עליו להשתמש כדי לאבטח מנה זו. מנהל התקן IPSec מבקש ש-ISAKMP (**I**nternet **S**ecurity **A**ssociation and **K**ey **M**anagement **P**rotocol) יישא וייתן לגבי שיטת אבטחה ומפתח אבטחה.

❖ ISAKMP נושא ונותן לגבי שיטת אבטחה ושולח אותה, כאשר מצורף אליה מפתח האבטחה למנהל התקן IPSec.

❖ השיטה והמפתח הופכים להיות שיוך האבטחה (**S**ecurity **A**ssociation ,SA) של IPSec. IPSec מאחסן את שיוך האבטחה במסד הנתונים שלו.

❖ שני המארחים המתקשרים צריכים להצפין ולפענח את תעבורת IP, כך שעל שניהם לדעת ולאחסן את שיוכי האבטחה.



תרשים 5.2 סקירת תהליך האבטחה של IP

ארכיטקטורת IPSec

יישום IPSec בסביבת Windows 2000 מתבצע באמצעות הרכיבים הבאים :

❖ סוכן מדיניות IPSec

❖ ISAKMP/Oakley Key Management Service

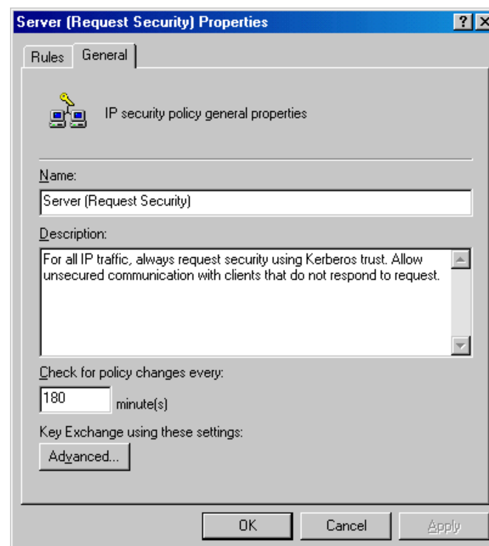
❖ מנהל התקן IPSec

❖ מודל IPSec

שירות סוכן מדיניות IPSec

סוכן המדיניות הוא מנגנון IPSec השוכן בכל מחשב מבוסס Windows 2000. סוכן המדיניות מופעל באופן אוטומטי כאשר מופעל המחשב. סוכן המדיניות מבצע את המשימות הבאות בכל פרק זמן המוגדר במדיניות IPSec, כפי שמתואר בתרשים 5.3:

1. מאחזר מ- Active Directory את מדיניות IPSec המשויכת למחשב זה.
2. אם לא משויכת למחשב מדיניות IPSec כלשהי, או אם הסוכן אינו מצליח להתחבר ל- Directory Service, הוא מנסה לקרוא את המדיניות מרישום המערכת (Registry) של המחשב. סוכן המדיניות מפסיק את פעולתו אם אינו מאתר מדיניות תואמת ב- Directory Service או ברישום המערכת.
3. אם אותרה מדיניות ב- Directory Service, העברת הנתונים של מידע המדיניות מ- Directory Service אל המחשב מוגנת באמצעות Data Integrity and Encryption Services.
4. שולח את מידע המדיניות למנהל ההתקן של IPSec, ל- ISAKMP/Oakley Key Management Service ולרישום המערכת.



תרשים 5.3 משימות המבוצעות על ידי סוכן המדיניות

ISAKMP/Oakley Key Management Service

שירות זה הוא מנגנון IPSec השוכן בכל מחשב הפועל בסביבת Windows 2000. לפני שניתן לשלוח צרורות נתוני IP ממחשב אחד למשנהו, חייב להיווצר שיוך אבטחה (Security Association, SA) בין שני המחשבים. SA הוא ערכת פרמטרים המגדירה את שירותי ומנגנוני האבטחה המשותפים בהם ייעשה שימוש לשם אבטחת ההתקשרות, כגון מפתחות ומאפייני אבטחה.

ISAKMP ממרכז את ניהול שיוך האבטחה, ומפחית בכך את משך ההתחברות. פרוטוקול Oakley מחולל את המפתחות המעשיים בהם ישתמשו הצדדים להצפנה ולפיענוח הנתונים המועברים. ISAKMP/Oakley מבצע פעולה בת שני שלבים :

1. מקים ערוץ מאובטח בין שני המחשבים לצורך ההתקשרות. כדי לבצע זאת הוא מאמת את זהויות המחשבים ומחליף נתוני מיפתוח כדי להשיג את המפתח הסודי המשותף בו ישתמשו המחשבים, כדי להצפין ולפענח את הנתונים.
2. מקים שיוך אבטחה בין שני המחשבים, אשר מועבר למנהל התקן IPSec יחד עם המפתח המשותף, בשני המחשבים, השולח והמקבל.

סוכן המדיניות מפעיל את שירות ISAKMP/Oakley באופן אוטומטי. שירות זה לא יופעל באופן אוטומטי או באופן ידני, אלא אם שירות סוכן המדיניות מופעל. אם לא ניתן להקים שיוך אבטחה, ניתן להגדיר את מדיניות IPSec שתבלום כל ניסיון התקשרות, או שתקבל התקשרות שאינה מאובטחת.

מנהל התקן IPSec

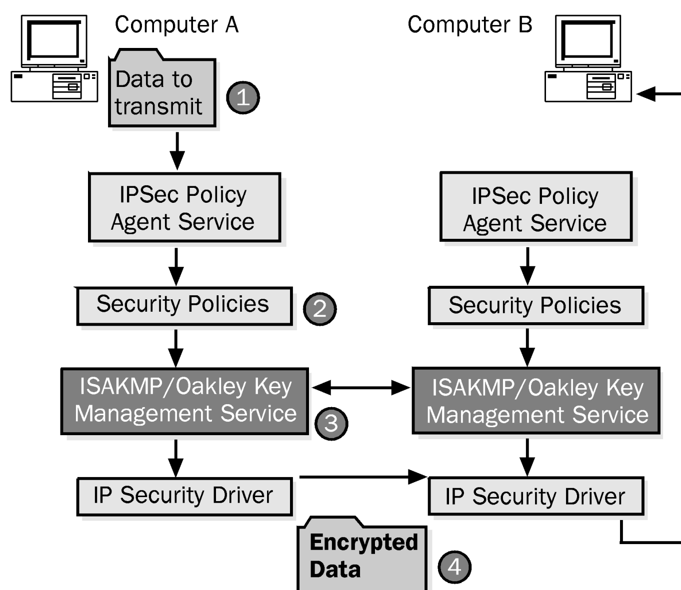
מנהל ההתקן של IPSec (IPSEC.SYS) שוכן בכל מחשב מבוסס Windows 2000. מנהל ההתקן עוקב אחר כל צרור נתוני IP (IP Datagram) ומנסה לאתר בו התאמה למסנן מרשימת מסננים שבמדיניות האבטחה של המחשב. רשימת המסננים מגדירה איזה מחשבים ורשתות דורשים תקשורת מאובטחת. אם אותרה התאמה למסנן, מנהל התקן IPSec במחשב השולח משתמש ב-SA ובמפתח המשותף, כדי להצפין מידע ולשלוח אותו למחשב המקבל. מנהל התקן IPSec במחשב המקבל מפענח את הנתונים שהתקבלו ומעביר אותם ליישום המקבל.

הערה סוכן המדיניות מפעיל את מנהל התקן IPSec באופן אוטומטי.

מודל IPSec

תרשים 5.4 מציג שני משתמשים במחשבים באינטראנט המפעילים Windows 2000 Server. גם למחשב A וגם למחשב B יש מדיניות IPSec פעילה.

1. דנה מפעילה יישום FTP ממארח A ושולחת נתונים לאורן, שיקבל אותם במארח B.
2. מנהל התקן IPSec במארח A מיידע את שירות ISAKMP/Oakley שלצורך התקשרות זו נדרש IPSec, תוך שימוש במדיניות שברישום המערכת אשר נרשמו שם על ידי סוכן המדיניות.
3. שירותי ISAKMP/Oakley במארח A ובמארח B מקימים מפתח משותף ושיוך אבטחה (SA).
4. מנהלי ההתקן IPSec במארח A ובמארח B מקבלים שניהם את המפתח ואת ה-SA.
5. מנהל התקן IPSec במארח A משתמש במפתח להצפנת הנתונים ושולח אותם למארח B.
6. מנהל התקן IPSec של מארח B מפענח את הנתונים ומעביר אותם ליישום המקבל, ממנו מאחזר אורן את הנתונים.



תרשים 5.4 תרשים זרימה של מדיניות IPSec להצפנה בין שני מחשבים

הערה הנתבים (Routers) והמתגים (Switches) שבנתיב, בין שני המחשבים המתקשרים, צריכים להשתתף רק בהעברת צרורות נתוני IP המוצפנים ליעדם. אבל, אם קיימת בין שני המחשבים גם חומת אש (Firewall), או שער אבטחה אחר, יש לאפשר העברת IP (IP Forwarding) או ליצור סינון מיוחד, כדי לאפשר העברה של צרורות נתוני IP מוצפנים.

שיקולים עבור IPSec

IPSec מספק הצפנה עבור מנות יוצאות, אך הוא עושה זאת על חשבון ביצועים. IPSec מיישם הצפנה סימטרית של נתוני רשת באופן יעיל מאוד. אבל, לשרתים התומכים במספר רב של חיבורים בו-זמניים, ההשפעה הנגרמת על הביצועים לצורך ביצוע ההצפנה היא מכבידה. בשל כך, עליך לתכנן ולבחון את IPSec תוך שימוש בהדמיית תעבורת רשת לפני שתיישם אותו. הבדיקה חשובה גם במקרה בו אתה משתמש בחומרה או תוכנה של צד-שלישי כדי לספק אבטחת IP. תוכל להגדיר מדיניות IPSec עבור כל Domain. תוכל להגדיר מדיניות IPSec כדי:

- ❖ לציין את סוגי האימות ואת רמות הסודיות הנדרשות בין לקוחות IPSec.
- ❖ לציין את רמת האבטחה הנמוכה ביותר המותרת לכל התקשרות בין לקוחות מודעי IPSec (IPSec-aware Clients).
- ❖ לאפשר או למנוע התקשרויות עם לקוחות שאינם מודעי IPSec.
- ❖ לדרוש שכל ההתקשרויות תהיינה מוצפנות לשם שמירה על סודיות, או לאפשר התקשרויות בטקסט פשוט.

שקול את השימוש ב-IPSec כדי לספק אבטחה ליישומים הבאים:

- התקשרויות Peer-to-Peer באינטראנט הארגוני, כגון: בין המחלקה המשפטית להנהלה.
- התקשרויות שרת/לקוח כדי להגן על מידע רגיש (סודי) המאוחסן בשרתים.
- התקשרויות בגישה מרחוק, בחיוג או באמצעות VPN (עבור התקשרויות VPN המשתמשות ב- Layer Two Tunneling Protocol, L2TP, זכור להגדיר מדיניות קבוצתית המאפשרת הרשמה אוטומטית לאישורי IPSec. למידע מפורט אודות אישורי מכונה להתקשרויות עבור L2TP over VPN, פנה למערכת העזרה של Windows 2000).
- התקשרויות WAN מאובטחות נתב-לנתב.

שקול את אסטרטגיות IPSec הבאות, בעת תכנון יישום האבטחה ברשת שלך:

- זהה איזה לקוחות ושרתים צריכים להשתמש בהתקשרויות IPSec.
- זהה אם אימות הלקוח מתבצע באמצעות סמיכות Kerberos, או באמצעות אישור דיגיטלי.
- תאר כל מדיניות IPSec, כולל כללים ורשימת מסננים.
- תאר שירותי אישורים הנדרשים לשם תמיכה באימות לקוחות באמצעות אישורים דיגיטליים.
- תאר את תהליך ההרשמה ואת האסטרטגיות להרשמת משתמשים לאישורי IPSec.

סיכום שיעור

IPSec היא סביבת עבודה של תקנים פתוחים להבטחת התקשרות פרטית מאובטחת ברשתות מבוססות IP, תוך שימוש בשירותי אבטחה בהצפנה. IPSec הוא שקוף למשתמש ומספק התקשרות מאובטחת ברמה גבוהה, בעלות נמוכה.

ארכיטקטורת IPSec מורכבת מארבעה מרכיבים עיקריים: סוכן המדיניות של IPSec, ISAKMP/Oakley Key Management Service, מנהל התקן IPSec ומודל IPSec.

שיעור 2: הגדרת IPSec

MMC (**M**icrosoft **M**anagement **C**onsole) יכול לשמש ליצירה ולהגדרה של מדיניות IPSec. הוא יכול לשמש לניהול מרוכז של מדיניות (עבור Active Directory), לנהל מדיניות באופן מקומי או לנהל מדיניות באופן מרוחק עבור מחשב. בשיעור זה תבחן את המסכים השונים המשמשים להגדרת IPSec. בנוסף, תיצור מדיניות אבטחת IP ניסיונית.

לאחר שיעור זה, תוכל

- לתאר כיצד ליישם IPSec.
- להגדיר מדיניות IPSec.
- לתאר את כרטיסיות המאפיינים השונות בתיבות **דו-שיח** IPSec Policy, Authentication Method, IP Packet Filtering, Filter Action **ומשימות** IPSec **נוספות**.

זמן לימוד משוער: 30 דקות

דרישות מקדימות ליישום IPSec

למחשבים ברשת שלך צריכה להיות מדיניות IPSec מוגדרת, אשר מתאימה לאסטרטגיית האבטחה הכוללת של הרשת שלך. מחשבים הנמצאים באותו Domain ניתן לארגן בקבוצות, ולהחיל את מדיניות IPSec על הקבוצות עצמן. ניתן ליצור מדיניות IPSec משלימה (Complementary IPSec Policy) עבור מחשבים שאינם באותו Domain, כדי לתמוך בתקשורת רשת מאובטחת.

כיצד ליישם IPSec

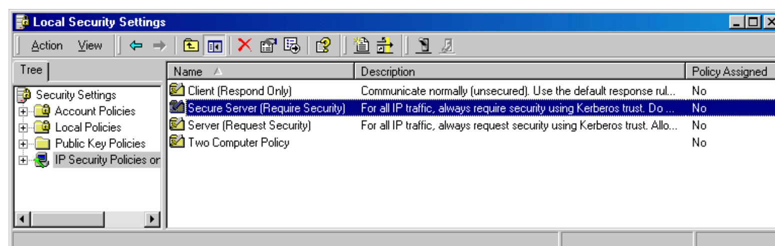
תוכל לצפות במדיניות אבטחת IP המהווה את ברירת המחדל באמצעות יישום ה-Snap-In של Group Policy, ב-MMC. המדיניות מופיעות תחת IP Security Policies ב-

Active Directory:Group Policy Object\Computer Configuration\Windows Settings\
IP Security Policies on Active Directory.

ניתן גם לצפות במדיניות IPSec ביישום Snap-In בשם IP Security Policy Management של MMC. כל מדיניות IPSec נשלטת על ידי כללים הקובעים מתי וכיצד יש להחיל את המדיניות. לחץ לחיצה ימנית על מדיניות, ומתפריט הקיצור בחר Properties. בכרטיסיה Rules מוצגת רשימה של כללי המדיניות. ניתן להמשיך ולחלק כללים לחלוקת משנה, וכך ליצור רשימת מסננים (Filter List), פעולות מסננים (Filter Action) ומאפיינים נוספים. יישום Snap-In של ברירת המחדל מופעל מתפריט Administrative Tools; דבר זה מאפשר הגדרת המחשב המקומי בלבד. כדי לנהל במרוכז מדיניות עבור מספר מחשבים, הוסף ל-MMC את ה-Snap-In של IP Security Management.

הגדרת מדיניות IPSec

חלון הפתיחה מציג שלוש רשומות מדיניות המוגדרות מראש: Client (Respond Only), Secure Server (Require Security) ו- Server (Request Security). כברירת מחדל, אף אחת ממדיניות אלו אינה פעילה. מדיניות אלו מוצגות בתרשים 5.5.



תרשים 5.5 MMC של Windows 2000 Member Server

ברירות מחדל אלו זהות, בין אם מדיניות IPSec היא מקומית ובין אם היא מאוחסנת ב- Active Directory, כחלק ממדיניות קבוצתית. במקרה המוצג כאן, המדיניות היא מקומית ב- Member Server.

❖ מדיניות Client (Respond Only) מאפשרת התקשרות בטקסט פשוט (Plaintext) אך תגיב לבקשות IPSec ותנסה לדון בנושא אבטחה. מדיניות זו מאפשרת ביעילות תקשורת טקסט-נקי (Clear-Text), אך תנסה לדון בנושא האבטחה במידה ומתבצעת בקשה לאבטחה. היא משתמשת ב- Kerberos V5 לצורך אימות.

❖ מדיניות Server (Request Security) גורמת לשרת לנסות ליצור התקשרות מאובטחת עבור כל שיח (Session). אם השיח נוצר על ידי לקוח שהוא אינו מודע-IPSec (IPSec-Aware), ההתקשרות תאופשר.

❖ מדיניות Secure Server (Require Security) דורשת סמכות Kerberos (Kerberos Trust) עבור כל מנות IP הנשלחות ממחשב זה, כאשר היוצאים מהכלל הן מנות שידור רחב (Broadcast), שידור מרובה (Multicast), Resource Reservation Setup Protocol (RSVP) ו-ISAKMP. מדיניות זו אינה מאפשרת התקשרות שאינה מאובטחת עם לקוחות. בשל כך, כל הלקוחות המתקשרים עם מחשב זה חייבים להיות מודעי-IPSec.

כדי לערוך מדיניות, לחץ עליה לחיצה ימנית ובחר Properties.

הערה ניתן לשייך רק מדיניות אחת בכל רגע נתון. אם הוגדרה מדיניות IPSec למספר מדיניות קבוצתיות חופפות, מיושמת היררכיית המדיניות הקבוצתית הרגילה.

סוגי חיבורים

ניתן לבחור בכרטיסיה Connection Type בתיבת דו-שיח Edit Rule Properties (ראה תרשים 5.6). כרטיסיה זו מוצגת גם כחלק מהאשף Rule Creation Wizard.

הערה ניתן להגדיר את כל הגדרות המדיניות באמצעות האשף. השימוש באשפים מופעל כברירת מחדל, אך ניתן להפסיק אותו על ידי ביטול הסימון בתיבת הסימון Use Add Wizard.



תרשים 5.6 תיבת דו-שיח Edit Rule Properties

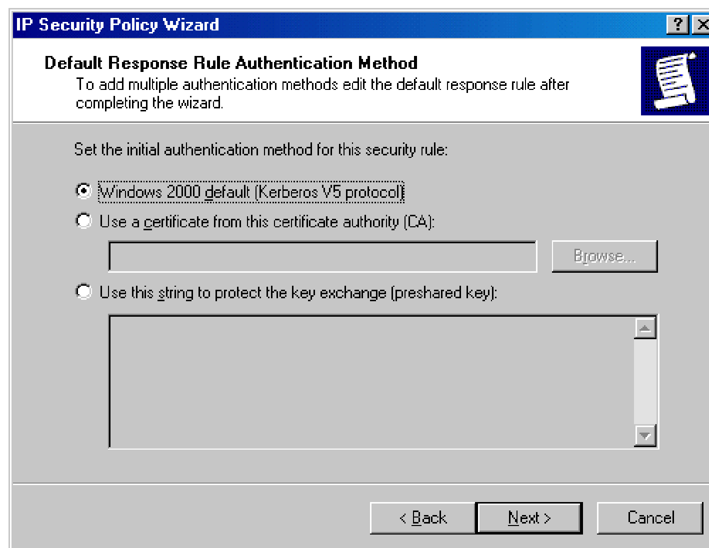
ציון סוג התחברות לכל כלל (Rule) יקבע איזה חיבור מחשב (מתאמי רשת או מודמים) יושפע ממדיניות IPSec. לכל כלל יש את מאפיין החיבור המציין האם הכלל חל על חיבור LAN, חיבור גישה מרחוק או כל חיבורי הרשת.

שיטת אימות

שיטת האימות מגדירה כיצד כל משתמש יהיה בטוח שהמחשבים או המשתמשים האחרים הם באמת מי שהם אומרים שהם. כפי שמתואר בתרשים 5.7, כל שיטת אימות מספקת את החלקים הנדרשים להבטחת הזהות. Windows 2000 תומכת בשיטות האימות הבאות:

- **Kerberos.** פרוטוקול האבטחה Kerberos V5 משמש בטכנולוגיית האימות המהווה את ברירת המחדל. פרוטוקול Kerberos מנפיק כרטיסים או תעודות אימות זהות וירטואליות, כאשר מחשב מתחבר ל-Trusted Domain. ניתן להשתמש בשיטה זו עבור כל לקוח המפעיל את פרוטוקול Kerberos V5 (בין אם הם לקוחות מבוססי-Windows, או לא) החבר ב-Trusted Domain.
- **Certificates.** אימות כזה דורש שתוגדר לפחות רשות מאשרת (CA, **C**ertificate **A**uthority) נסמכת אחת. Windows 2000 תומכת באישורים של X.509 Version 3, כולל אישורי CA שהונפקו על ידי רשויות מאשרות מסחריות. כלל עשוי לציין מספר שיטות אימות. דבר זה מבטיח שתימצא שיטה משותפת, כאשר מתבצע המשא ומתן עם העמית.

❖ **Preshared Key.** זהו מפתח משותף סודי, המוסכם בין שני משתמשים. זו דרך קלה לשימוש ואשר אינה דורשת מהלקוח להפעיל את פרוטוקול Kerberos V5, או שיהיה לו אישור מפתח ציבורי. כדי להשתמש במפתח משותף זה, חייבים שני הצדדים להגדיר IPSec באופן ידני. זוהי שיטה פשוטה לאימות מארחים שאינם מבוססי-Windows ומארחים עצמאיים (Stand-alone Host).



תרשים 5.7 תיבת דו-שיח Default Response Rule Authentication Method

---

הערה המפתח הנגזר מהאימות הוא לצרכי אימות **בלבד**; הוא **אינו** המפתח המשמש להצפנה או לאימות הנתונים.

לכל כלל יכולה להיות מוגדרת שיטת אימות אחת או יותר. כל שיטת אימות מוגדרת מופיעה ברשימה, על פי סדר עדיפותן. אם לא ניתן להשתמש בשיטה הראשונה, יתבצע ניסיון באמצעות השיטה הבאה.

סינון מנות IP

אבטחת IP מיושמת על מנות כאשר הן נשלחות או מתקבלות. המנות מושוות למסננים כאשר הן נשלחות (Outbound), כדי לבחון אם יש לאבטח אותן, לחסום אותן או להעביר אותן כטקסט פשוט. המנות מושוות למסננים כאשר הן מגיעות (Inbound), כדי לבחון שוב אם יש לדון בנושא האבטחה, או אם יש לחסום אותן או לאפשר את העברתן אל המערכת.

מפרטי סינון יחידים מקובצים להם יחדיו לרשימת מסננים (Filter List), כדי לאפשר לתבנית מורכבת יותר של תעבורה להיות מקובצת ומנוהלת כרשימת מסננים יחידה, כמו למשל **שרתי קבצים בניין 7** או **תעבורה חסומה**. ניתן לשתף רשימות מסננים לפי הצורך בין כללי IPSec השונים, באותה מדיניות או במדיניות IPSec אחרות. ניתן להגדיר את מפרטי המסננים לתעבורה נכנסת או לתעבורה יוצאת.

❖ מסנני כניסה, המיושמים על תעבורה נכנסת, מאפשרים למחשב המקבל להשוות את התעבורה עם רשימת מסנני ה-IP, להגיב לבקשות לגבי תקשורת מאובטחת או להשוות את התעבורה עם SA קיים ולפענח את המנות המאובטחות.

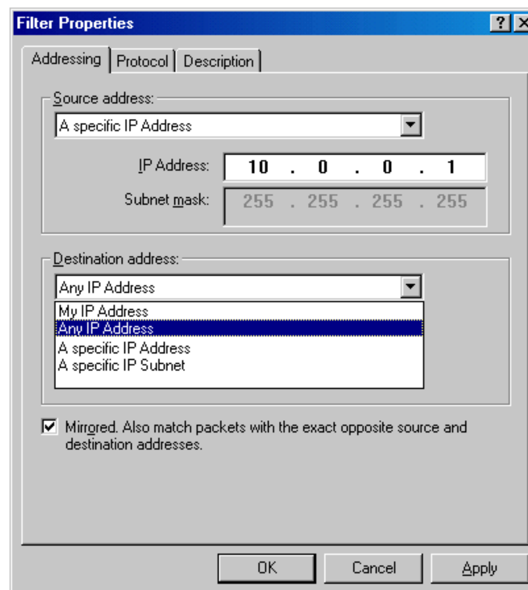
❖ מסנני יציאה, המיושמים על תעבורה היוצאת מהמחשב לכיוון היעד, מזניקים מו״מ אבטחה שחייב להתבצע ולהסתיים לפני שהתעבורה נשלחת.

חשוב למרות שמסנני יציאה וכניסה מוגדרים ומשמשים ברשימת מסננים, אין זה ברור בממשק המשתמש איזה מסנן נוצר. כתובות המקור והיעד הן הקובעות אם המסנן הוא מסנן כניסה (Inbound) או מסנן יציאה (Outbound).

חייב להיות מסנן המכסה את כל תרחישי התעבורה האפשריים לגביהם חל הכלל המשויך. מסנן כולל את הפרמטרים הבאים:

1. כתובת היעד וכתובת המקור של מנת ה-IP. כפי שניתן לראות בתרשים 5.8, כאשר יוצרים או עורכים מסנן, ניתן לבחור מבין אפשרויות הכתובת הבאות:

❖ **My IP Address**	כתובת ה-IP של המחשב המקומי.
❖ **Any IP Address**	כתובת Unicast בלבד. IPSec אינו תומך ב-Multicast או Broadcast.
❖ **A Specific IP Address**	זו כתובת IP מסוימת ברשת המקומית, או באינטרנט.
❖ **A Specific IP Subnet**	כולל את כל כתובות ה-IP ברשת משנה המצוינת.



תרשים 5.8 תיבת דו-שיח Filter Properties של מנת IP

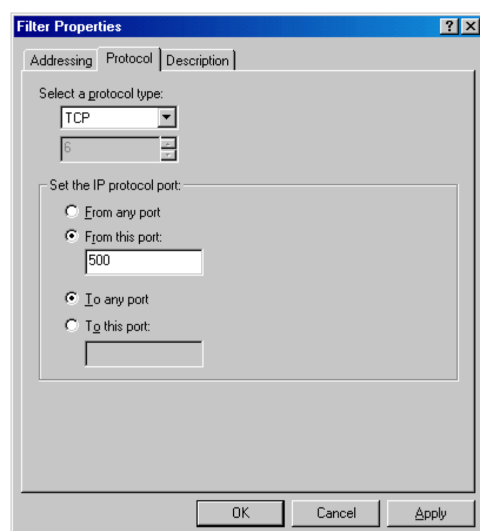
הערה IPSec מאכלס את My IP Address עם כתובת ה-IP המאוגדת הראשונה. אם במערכת מותקן יותר מאשר מתאם רשת יחיד (Multihome System), IPSec ישתמש רק באחת מהכתובות IP, לא בשתיהן. לקוחות RRAS (Routing and Remote Access) נחשבים למערכות Multihome, ולכן ייתכן ש-IPSec לא ירשום נכון את הכתובות.

2. הפרוטוקול באמצעותו נשלחת המנה. כברירת מחדל מוגדרים כל פרוטוקולי הלקוח של IP הנכללים בחבילת הפרוטוקולים TCP/IP.

טבלה 5.1 מציגה רשימה של סוגי הפרוטוקולים הזמינים בכרטיסיה Protocol שבתיבת דו-שיח Filter Properties המתוארת בתרשים 5.9.

טבלה 5.1 סינון פרוטוקולים

סוג פרוטוקול	תיאור
ANY	כל פרוטוקול
EGP	Exterior Gateway Protocol
HMP	Host Monitoring Protocol
ICMP	Internet Control Message Protocol
Other	פרוטוקול שאינו מוגדר, המבוסס על מספר פרוטוקול IP
RAW	נתונים גולמיים מעל IP
RDP	Reliable Datagram Protocol
RVD	MIT Remote Virtual Disk
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
XNS-IDP	Xerox NS IDP



תרשים 5.9 תיבת דו-שיח
Filter Properties

3. יציאת (Port) המקור והיעד של הפרוטוקול עבור TCP ו-UDP. גם כאן ברירת המחדל כוללת את כל היציאות, אך ניתן להגדיר יישום רק על מנות הנשלחות או מתקבלות ביציאה (Port) מסוימת.

בחר את מאפייני המסנן כאשר אתה עורך או יוצר מסנן. ניתן לנהל מסננים באופן גלובלי, על ידי לחיצה ימנית על המחשב המנוהל בחלונית השמאלית. ניתן גם לנהל אותם מתוך כל אחת מהכרטיסיות Rule Properties שבמדיניות. האשף Filter Creation Wizard מאפשר להגדיר מאפיינים אלה.

שיקוף

שיקוף (Mirroring) מאפשר למסנן להשוות מנות עם כתובות יעד ומקור הפוכות לגמרי. מסנן יציאה (Outbound Filter), אשר מציין את כתובת ה-IP ככתובת המקור ואת המחשב השני ככתובת היעד, ייצור באופן אוטומטי מסנן כניסה (Inbound Filter) בו מוגדר המחשב השני ככתובת המקור וכתובת ה-IP של המחשב היוזם ככתובת היעד.

הערה למעשה, המסנן המשוקף אינו מופיע ברשימת המסננים. במקום זאת, תהיה תיבת הסימון Mirrored שבתיבת דו-שיח Filter Properties, מסומנת.

אם מארח A מעוניין להחליף מידע עם מארח B תמיד באופן מאובטח.

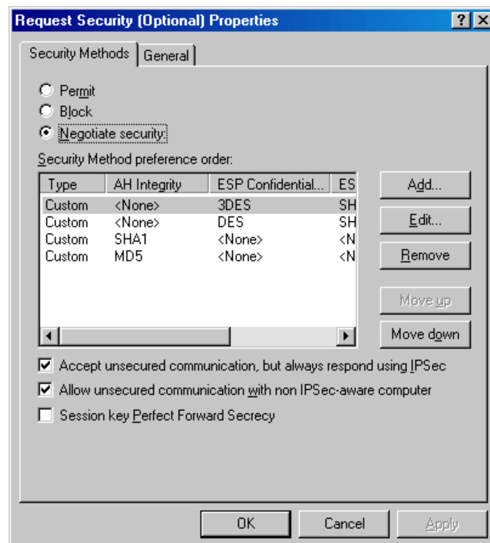
- כדי לשלוח נתונים מאובטחים למארח B, חייבת מדיניות IPSec של מארח A לכלול מפרט סינון עבור כל המנות היוצאות אל מארח B.
- כדי לקבל נתונים מאובטחים ממארח A, חייבת מדיניות IPSec של מארח B לכלול מפרט סינון עבור כל מנה המגיעה מאת מארח A, או שהיא חייבת שתהיה לה מדיניות בה מוגדר כלל תגובת-ברירת-מחדל (Default-Response) כפעיל (Active).
- שיקוף (Mirroring) יאפשר לכל מארח לשלוח או לקבל נתונים מהמארח האחר, מבלי ליצור מסננים נוספים לשם כך.

פעולות מסנן

פעולת המסנן קובעת איזו פעילות אבטחה תינקט ברגע שהופעל המסנן. הפעולה (Action) מציינת האם לבלום (Block) את התעבורה, לאפשר אותה או לנהל מו״מ בנוגע לאבטחת חיבור זה. המשא ומתן כולל תמיכה אך ורק עבור אמיתות ושלמות, תוך שימוש בפרוטוקול כותרת האימות (AH), או עבור שלמות וסודיות, תוך שימוש בפרוטוקול **E**ncapsulating **S**ecurity **P**ayload (ESP). ניתן להתאים באופן אישי כל פעולת מסנן, מה שמאפשר למנהל הרשת את האפשרות לבחור לאיזה פרוטוקולים נדרש אימות ולאיזה פרוטוקולים נדרשת סודיות.

ניתן להגדיר פעולת מסנן אחת או יותר. כפי שניתן לראות בתרשים 5.10, פעולות המסנן מופיעות כרשימה, כאשר השיטה הראשונה הנרשמת מקבלת קדימות. אם אין אפשרות לבצע פעולת מסנן זו, ייערך ניסיון להפעיל את פעולת המסנן הבאה.

ניתן גם לבחור רמת אבטחה גבוהה או בנונית, במקום להגדיר שיטה מותאמת באופן אישי. אבטחה ברמה גבוהה גם מצפינה וגם מבטיחה את שלמות הנתונים. אבטחה ברמה בינונית רק מבטיחה את שלמות הנתונים.



תרשים 5.10 מאפייני מדיניות
Secure Initiator Negotiation

משימות IPSec נוספות

בפני מנהל המערכת עומדות מספר משימות נוספות, אליהן ניתן להגיע על ידי לחיצה ימנית על סמל IP Security Policy שבחלון השמאלי. משימות אלו כוללות את:

- **Manage IP Filter Lists and Filter Actions.** משימה זו מאפשרת למנהל המערכת להגדיר מסננים ופעולות מסננים בנפרד מכללים יחידים. לאחר שנוצר כלל (Rule) ניתן להפעיל את המסננים או את פעולות המסננים, כפי שמתואר בתרשים 5.11.

- **Check Policy Integrity.** מכיון ש- Active Directory מתייחס למידע האחרון שנשמר כאל מידע עדכני, אם מספר מנהלי מערכת (Administrators) עורכים מדיניות, עלולים הקישורים שבין רכיבי המדיניות להינתק. למשל:

  מדיניות A משתמשת במסנן A

  מדיניות B משתמשת במסנן B

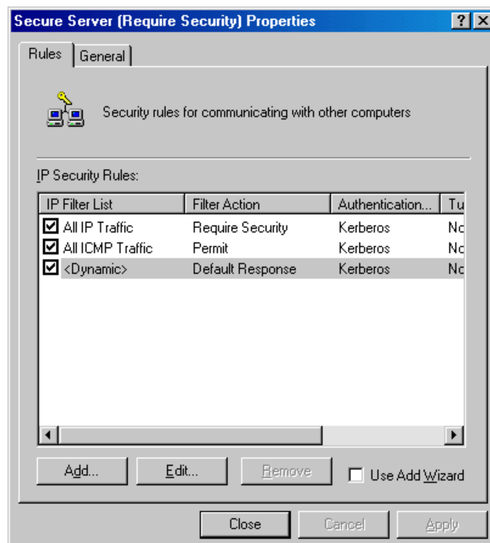
  זאת אומרת שמסנן A קשור למדיניות A ואילו מסנן B קשור למדיניות B.

  נניח שאורון עורך את מדיניות A ומוסיף לה כלל להשתמש במסנן C.

  בו בזמן עורכת תמי את מדיניות B ממיקום שונה, ומוסיפה כלל שגם הוא משתמש במסנן C.

  אם שניהם שומרים את השינויים בו-זמנית, יוכל מסנן C להיות מקושר הן למדיניות A והן למדיניות B; אבל, מקרית כגון זו היא דבר נדיר. במקום זאת, אם מדיניות A נשמרה אחרונה, היא תדרוס את הקישור שבין מדיניות B למסנן C. מסנן C יהיה

קשור רק למדיניות A. הדבר יגרום לבעיות בעתיד, כאשר מסנן C יעודכן, מפני שמשתמשי מדיניות A יקבלו את השינויים, אבל משתמשי מדיניות B לא.



תרשים 5.11 הכרטיסיה Rules

בדיקת התקינות (Integrity Check) של המדיניות מונעת מבעיה זו להתרחש, על ידי וידוא הקישורים בכל מדיניות IPSec. רצוי להפעיל את בדיקת התקינות לאחר ביצוע שינויים למדיניות. משימות אחרות הזמינות למנהלי המערכת נגישות גם הן על ידי לחיצה ימנית על סמל IP Security Policy בחלון השמאלי. משימות אלו מתוארות ברשימה הבאה:

- **Restore Default Policies** משחזר את המדיניות המוגדרות מראש להגדרותיהן הראשוניות.
- **Import Policies** מאפשר ייבוא מדיניות ממארח אחר ברשת.
- **Export Policies** מאפשר ייצוא מדיניות למארח אחר ברשת.

תרגול: בדיקת IPSec

בתרגול זה תפעיל מדיניות מובנית של IPSec, כדי לראות שהיא חוסמת התקשרויות אם התעבורה אינה יכולה להיות מאובטחת. אם שני מחשבים הפועלים בסביבת Windows 2000 Server חברים באותם תחומי Windows 2000 Server, או שהם בתחומים נסמכים (Trusted Domains), אז ניתן להשתמש במדיניות IPSec המובנות כדי להקים התקשרות מאובטחת בקלות יתרה. אחרת, לצורך הבדיקה, תצטרך להגדיר מדיניות IPSec משלך בכל מחשב, בהתאם לצעדים המפורטים בסעיפים הבאים.

לפני שתמשיך עם שיעור זה, הפעל את קובץ ההדגמה Ch05.exe שבתקליטור המצורף לספר זה (בתיקיה Media). הקובץ מתאר את אופן בדיקת IPSec.

➢ **כדי לבחון התקשרויות עם מחשב אחר**

1. בצע PING לכתובת ה-IP של המחשב האחר.

אתה אמור לקבל ארבע תגובות ל-PING. תגובות אלו מוודאות שאתה יכול לתקשר עם המחשב האחר.

➢ **כדי להוסיף את IPSec ל-MMC**

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ובחר Local Security Policy MMC Plug-in.
2. בחר את IP security policies on local machine בחלונית השמאלית.
3. בחלונית הימנית, לחץ לחיצה ימנית על Secure Server (Require Security), ובחר Properties.
4. בתיבת דו-שיח Secure Server (Require Security) Properties לחץ Add. על המסך מופיע Security Rule Wizard.
5. במסך הראשון Welcome לחץ Next.
6. במסך Tunnel Endpoint לחץ Next.
7. במסך Network Type לחץ Next.
8. במסך Authentication Method, לחץ על לחצן האפשרויות Use this string to protect the key exchange (Preshared Key). הקלד את המחרוזת MSPRESS בתיבת הרשימה הנפתחת, ולחץ Next.
9. לחץ על All IP traffic, ובמסך IP Filter List לחץ Next.
10. לחץ על Require Security, ובמסך Filter Action לחץ Next.
11. לחץ Finish כדי לסגור את האשף.
12. כעת, משהוספת רשימת מסננים מגבילים, בטל את בחירת כל רשימות המסננים הנבחרות כברירת מחדל.
13. סגור את תיבת דו-שיח Secure Server (Require Security) Properties.
14. לחץ לחיצה ימנית על Secure Server (Require Security) ומתפריט הקיצור בחר Assign.
15. בצע PING למחשב השני. שים לב לכך שפעולה ה-PING לא הצליחה.
16. כדי לאפשר לעצמך לתקשר עם הרשת מחדש, בטל (Unassign) את המדיניות Secure Server (Require Security) באמצעות תפריט הקיצור.

סיכום שיעור

Windows 2000 מגיעה כשמוגדרות בה שלוש מדיניות: Client (Response Only), Server (Request Security) ו- Secure Server (Require Security). ניתן לשנות מדיניות אלו או להסירן, בכל עת. יתר על כן, ניתן אף להוסיף מדיניות מותאמות באופן אישי. תוך שימוש ב-IPSec יכולה Windows 2000 לתמוך במיגוון שיטות לאימות מארחים ולספק סינון מנות IP, ועל ידי כך גם לאפשר למחשבים לתקשר או למנוע התקשרות, בהתבסס על מיגוון רחב של כללים ומסננים.

שיעור 3: התאמה אישית של מדיניות וכללי IPSec

ניתן להתאים את מדיניות וכללי IPSec די בקלות. בשיעור זה תסקור את הדרכים לאבטחת הרשת שלך תוך שימוש במיגוון השיטות המתואר, תוך התחשבות בגורמים כגון שרתי Proxy, תרגומי כתובות רשת (NAT, **N**etwork **A**ddress **T**ranslation), SNMP, DHCP, DNS, WINS ו-Domain Controllers.

לאחר שיעור זה, תוכל

- להסביר את מדיניות וכללי IPSec.
- לתאר כיצד להגדיר את IPSec לשימוש עם Firewall, NAT ושרתי Proxy.
- לתאר את השימוש ב-IPSec לאבטחת רשת עם SNMP, DHCP, DNS, WINS או DCs.

זמן לימוד משוער: 40 דקות

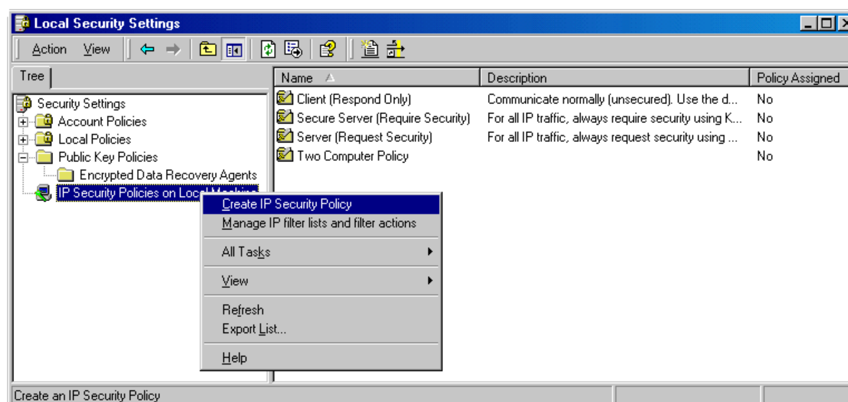
אבטחה מבוססת מדיניות

שיטות אבטחה הדוקה המבוססות על קריפטוגרפיה (הצפנה) אמנם הפכו לנחוצות כדי להגן על תקשורת, אך הן עלולות גם להגדיל באופן משמעותי את עומס ניהול המערכת. IPSec מפחית עומס זה על ידי שהוא מספק ניהול מבוסס-מדיניות. מנהל האבטחה ברשת שלך יכול להגדיר מדיניות IPSec כך שתתאמנה לדרישות המשתמש, הקבוצה, היישום, ה- Domain, ה-Site או הארגון בכלל. Windows 2000 מספקת ממשק ניהול, שנקרא IPSec Policy Management, באמצעותו ניתן להגדיר מדיניות IPSec עבור מחשבים בודדים או קבוצות של מחשבים בתוך Active Directory.

מדיניות IPSec

מדיניות IPSec (IPSec Policy) הוא שם כולל עבור קבוצת כללים והגדרות לחילופי מפתחות. ניתן להחיל את המדיניות כמדיניות לאבטחת Domain או כמדיניות להגנה על מחשב בודד. מחשב ב-Domain יירש באופן אוטומטי את מדיניות IPSec המשויכת למדיניות אבטחת ה-Domain, כאשר הוא מתחבר (Log on) ל-Domain. אם מחשב אינו מחובר ל-Domain (למשל, מחשב נייד או שרת עצמאי), מאוחסנת ומאוחזרת מדיניות IPSec מרישום המערכת (Registry) של המחשב.

דבר זה מאפשר גמישות גדולה בהגדרת מדיניות אבטחה לקבוצות של מחשבים דומים, או מחשבים בודדים להם דרישות מיוחדות. לדוגמה, ניתן להגדיר מדיניות אבטחה אחת עבור כל המשתמשים באותה רשת, או לכל המשתמשים במחלקה מסוימת. מדיניות IPSec נוצרות באמצעות יישום Snap-In בשם IPSec Management, כפי שנראה בתרשים 5.12, עבור Windows 2000 Member Server.



תרשים 5.12 MMC ובו Windows 2000 Member Server

כללים

כללים (Rules) שולטים בביצוד ומתי יש להשתמש ב-IPSec. כלל מכיל רשימה של מסנני IP (IP Filter) ומציין את פעולות האבטחה בהן יש לנקוט, כאשר נמצאת התאמה למסנן כלשהו. כלל הוא אוסף של:

- ❖ מסנני IP
- ❖ מדיניות ניהול משא ומתן
- ❖ שיטות אימות
- ❖ תכונות תיעול של IP
- ❖ סוגי מתאמים

כל מדיניות אבטחה יכולה להכיל מספר מרובה של כללים. דבר זה מאפשר גמישות רבה יותר בשיוך מדיניות IPSec אחת למספר מחשבים, עם תרחישי התקשרות שונים. למשל, מדיניות אחת עשויה לכלול את כל המשתמשים במחלקה או רשת, אבל ייתכן שיידרשו מספר כללים עבורה: אחד לתקשורת אינטראנטית ואחר עבור תקשורת אינטרנטית הדורשת תיעול (Tunneling).

מסנני IP ומפרטי מסנן

כל הכללים מבוססים על התאמה בין מנות לבין מסנני IP. כל כלל יכול שיהיה לו מסנן IP אחד פעיל. מנהל ההתקן של IPSec (IPSec Driver) בוחן כל צרור נתוני IP ומחפש התאמה למסנן IP הפעיל. אם נמצאה התאמה, הפעולה המצוינת בכלל המשויך מיושמת על תקשורת זו.

מפרטי מסנן

צרורות נתוני IP (IP Datagram) נבדקות לאיתור התאמה לכל מפרט מסנן. מפרט מסנן (Filter Specification) מכיל את המאפיינים הבאים:

- ❖ כתובת המקור וכתובת היעד של צרור נתוני IP, מבוסס על כתובת IP, שם DNS או על רשת או רשת משנה מסוימים.
- ❖ פרוטוקול, TCP או UDP.
- ❖ מספרי יציאת הפרוטוקול המסוימים של המקור ושל היעד עבור TCP או UDP.

שיטות אבטחה ומדיניות ניהול משא ומתן

רמת האבטחה המשמשת להתקשרות נקבעת על פי שיטות האבטחה (Security Method) ומדיניות ניהול המשא ומתן (Negotiation Policy).

שיטות אבטחה

כל שיטת אבטחה (Security Method) מציינת רמה ייחודית של אבטחה בה יש להשתמש לשם התקשרות. מדיניות ניהול משא ומתן אחת יכולה להכיל מספר מרובה של שיטות אבטחה, וזאת כדי להגדיל את האפשרות ששני מחשבים ימצאו שיטת אבטחה משותפת. שירות ISAKMP/Oakley בכל מחשב בוחן את רשימת שיטות האבטחה בסדר יורד, עד להימצאותה של שיטת אבטחה משותפת. תוכל לבחור בין שיטות אבטחה המוגדרות מראש לבין שיטות אבטחה שתיצור בעצמך:

- ❖ **High.** IP ESP מספק שירותי סודיות, שלמות, אימות והגנה מפני שידור חוזר.
- ❖ **Medium.** פרוטוקול האבטחה IP AH מספק שירותי שלמות, אימות והגנה מפני שידור חוזר. סודיות אינה חלק מ-AH.
- ❖ **Custom.** בנוסף לבחירה בין ESP ו-AH, משתמשים מנוסים יכולים לציין אלגוריתם לאימות, שלמות וסודיות.

מדיניות ניהול משא ומתן

מדיניות ניהול משא ומתן (Negotiation Policy) הוא שם עבור אוסף שיטות אבטחה. ניתן להגדיר מדיניות ניהול משא ומתן פעילה יחידה לכל כלל. אם לא ניתן להגיע להסכמה על שיטת האבטחה משותפת בין שני מחשבים ניתן להגדיר את מדיניות ניהול המשא ומתן כך שתמנע התקשרות עם מחשב זה, או שתשלח את הנתונים נקיים (ללא הצפנה).

מכיון ש-IPSec אינו מפריע לכותרת IP המקורית, הוא ייחשב כתעבורת IP רגילה וינותב בהתאם. הדבר נכון גם לגבי מצבי תיעול (Tunneling) ותעבורה (Transport).

ESP ונתבים

ESP אינו מצפין ואינו מאמת כותרות IP, ומשאיר אותן כמות שהן. אפילו במצב תיעול (Tunnel Mode), בו כותרת IP המקורית מוצפנת, ניתוב אינו מהווה בעיה. כותרת IP

המתועלת החדשה (שנותרה ללא שינוי) משמשת לניתוב בין נקודות הקצה של התעלה. לאחר שהמנה הגיעה לנקודת היעד בקצה התעלה, היא מאומתת ומפוענחת. מנת IP המקורית מועברת ללא אימות או הצפנת IPSec ליעדה הסופי.

AH ונתבים

AH משתמש בכל השדות שבכותרת IP כדי ליצור את ICV (**I**ntegrity **C**heck **V**alue). מאחר ונתבים משנים את השדות בכותרת ה-IP הדבר עלול להוות בעיה מסוימת; אבל, אותם שדות שייתכן שישונו, מקבלים את הערך 0 (אפס) לצורך חישוב ה-ICV. בשל כך, הנתבים יכולים לשנות את אותם שדות ברי-שינוי (TTL [**T**ime-**T**o-**L**ive], checksum וכדומה) מבלי להשפיע על חישובי ICV. בצד המקבל, נותן IPSec לשדות פעם נוספת את הערך 0, כדי לבצע את חישובי ICV.

הדבר נכון גם לגבי מצב תיעול, בו כותרת IP החדשה של התעלה תשמש לחישובי ICV, אך אותם שדות ברי-שינוי יקבלו את הערך 0. בנקודת היעד של קצה התעלה נבחן ה-Hash ומנת ה-IP המקורית מועברת ללא אימות נוסף.

IPSec דרך חומות אש

כל נתב (Router) או מתג (Switch) שבנתיב הנתונים שבין המארחים המתקשרים, פשוט יעביר את מנות ה-IP המוצפנות ו/או מאומתות ליעדן. אבל, אם בדרך יימצא נתב מסנן (Filtering Router) או חומת אש (Firewall), יש לאפשר העברת IP (IP Forwarding) עבור פרוטוקולי IP הבאים ויציאות UDP (UDP Port):

- **IP Protocol ID of 51**. שני המסננים, היוצא והנכנס, צריכים להיות מוגדרים כך שיאפשרו תעבורת AH.
- **IP Protocol ID of 50**. שני המסננים, היוצא והנכנס, צריכים להיות מוגדרים כך שיאפשרו תעבורת ESP.
- **UDP port 500**. שני המסננים, היוצא והנכנס, צריכים להיות מוגדרים כך שיאפשרו תעבורת ISAKMP.

שים לב לכך שהגדרות אלו תשמשנה כדי לאפשר לתעבורת IPSec לעבור דרך חומת האש רק בעת השימוש במצב תעבורה (Transport Mode), או במידה וחומת האש היא מצידו הציבורי של שרת התיעול (Tunnel Server). לא ניתן להשתמש ב-IPSec באותו אופן בו תיישם חומת האש את IPSec על כל המנות הנכנסות או היוצאות. הנתב יצטרך ליצור ולשמר את כל ה-SA המשויכים לכל התקשרות.

הערה סינון חומת אש המקובל (סינון ביציאות TCP ו-UDP) אינו יכול להתבצע על תעבורת ESP, מפני שמספרי היציאות מוצפנים.

IPSec דרך NAT או Proxy

לא ניתן להשתמש ב-IPSec דרך NAT או יישומי Proxy. למרות העובדה, שכותרת ה-IP נשארת ללא שינוי, ההצפנה והאימות אינם מאפשרים ביצוע שינויים בשדות האחרים.

NAT

הסעיפים הבאים ידונו בשאלה מדוע IPSec אינו עובד דרך NAT.

חוסר היכולת להבחין בין שטפי נתונים מרובים של נתוני IPSec

כותרת ESP מכילה את SPI (**S**ecurity **P**arameters **I**ndex), מדד פרמטר האבטחה). SPI משמש יחד עם כתובת IP של היעד בכותרת IP רגילה ובכותרת IPSec, כדי לזהות SA של IPSec.

עבור תעבורה היוצאת משער NAT (NAT Gateway), כתובת IP של היעד נשארת ללא שינוי, אך לא כן כתובת IP של המקור. עבור תעבורה הנכנסת ל-NAT, יש למפות את כתובת היעד לכתובת IP פרטית. כדי ש-IPSec יעבוד כהלכה, יש צורך למפות גם את ה-SPI (מדד פרמטר האבטחה). למרות שניתן למפות את SPI, ידרוש הדבר ביצוע שינוי בשדה SPI. אם השדה SPI ישונה, יהיו חישובי ה-ICV לא תקינים.

הדבר נכון גם לגבי AH, בו SPI הוא חלק מ-AH ומשמש לחישובי ICV.

חוסר היכולת לשנות את סכומי הביקורת של TCP ו-UDP

כותרות TCP ו-UDP מכילות סכום ביקורת (Checksum) הכולל את כתובת המקור ואת כתובת היעד של כותרת IP רגילה. הכתובות בכותרת IP הרגילה אינן ניתנות לשינוי מבלי לפגוע בסכום הביקורת שבכותרות TCP ו-UDP, ובכך להפוך אותו ללא חוקי. בשל כך, NAT אינו יכול לעדכן את כותרות UDP ו-TCP, מפני שהן נמצאות בחלק המוצפן של ה-ESP, או שנעשה בהן שימוש בחישובי ICV.

יישומי Proxy

מכיון שיישומי Proxy פועלים בשכבת היישום (Application Layer) עליהם להיות מודעי-IPSec (IPSec-Aware), וצריך שיהיה להם שיוך אבטחה עבור כל לקוח IPSec. לכל הדעות, הדבר אינו הגיוני ואפשרות זו אינה מסופקת עם יישומי Proxy.

שיקולים נוספים של IPSec

בסעיף זה תלמד אודות שיקולי הגדרה נוספים של IPSec. בין השאר ידובר על תקשורת מאובטחת באמצעות SNMP והפעלת שירותי שרת, כגון DNS ו-WINS.

אבטחת SNMP

כל המערכות בהן SNMP פעיל, חייבות להיות מוגדרות לשימוש ב-IPSec, או לפחות שמדיניות IPSec תוגדר כך שהיא תאפשר התקשרות לא מאובטחת, במידה ונוצר מצב בו כל המארחים בהם SNMP פעיל **אינם** יכולים ש**גם** IPSec יהיה פעיל. אחרת, תקשורת מאובטחת לא תתקיים והודעות SNMP לא תשודרנה.

IPSec אינו מצפין את פרוטוקול SNMP באופן אוטומטי. היוצאות מהכלל היחידות הן המדיניות המוגדרות מראש Secure Initiator ו- Lockdown, המוגדרות לאבטח גם תעבורת SNMP. כדי לאבטח SNMP, הוסף שני צמדים של מפרטי מסנן למדיניות חדשה או קיימת במארח בו SNMP פעיל (SNMP-Enabled Host).

הצמד הראשון יהיה עבור תעבורת SNMP רגילה (הודעות SNMP) ויכלול מפרט ראשון עבור מסנן כניסה אחד ומפרט שני עבור מסנן יציאה אחד.

➢ **בכרטיסיה Addressing שבתיבת דו-שיח IP Filter List**

1. קבע את הכתובת Source לכתובת ה-IP של מערכת ניהול ה-SNMP.
2. קבע את הכתובת Destination כ- My IP Address, מה שיתרגם את כתובת ה-IP לזו של המארח אליו משויכת המדיניות (סוכן SNMP).
3. סמן את Mirrored כדי שייצור באופן אוטומטי את מפרט מסנן היציאה.

➢ **בכרטיסיה Protocol שבתיבת דו-שיח IP Filter List**

1. קבע את Protocol Type כ-TCP או UDP (אם שניהם נדרשים, צור מפרט מסנן נוסף).
2. בתיבות From this port ו- To this port קבע את הערך 161.

צמד מפרטי המסנן השני יהיה עבור לכידת הודעות SNMP ויכלול גם מפרט עבור מסנן כניסה אחד ומפרט נוסף עבור מסנן יציאה אחד.

➢ **בכרטיסיה Addressing שבתיבת דו-שיח IP Filter List**

1. קבע את הכתובת Source לכתובת ה-IP של מערכת ניהול ה-SNMP.
2. קבע את הכתובת Destination כ- My IP Address, מה שיתרגם את כתובת ה-IP לזו של המארח אליו משויכת המדיניות (סוכן SNMP).
3. סמן את Mirrored כדי שייצור באופן אוטומטי את מפרט מסנן היציאה.

➢ **בכרטיסיה Protocol שבתיבת דו-שיח IP Filter List**

1. קבע את Protocol Type כ-TCP או UDP (אם שניהם נדרשים, צור מפרט מסנן נוסף).
2. בתיבות From this port ו- To this port קבע את הערך 162.

מערכת הניהול של SNMP או ה-MMC חייבים להיות שניהם מודעי-IPSec (IPSec-Aware). שירות SNMP בסביבת Windows 2000 תומך בתוכנת ניהול SNMP, אך כיום אינו כולל תוכנה מסוג זה. כדי לאבטח תעבורת SNMP באמצעות IPSec צריכה תוכנת הניהול של צד-שלישי לאפשר IPSec.

שרתי DHCP, DNS, WINS או DCs

אם אתה מאפשר IPSec עבור שרת המפעיל איזה מבין שירותים אלה, בדוק אם בכל הלקוחות שלהם IPSec אפשרי. ודא שהמדיניות, ובעיקר הגדרות האימות וניהול המשא ומתן, תואמות. אחרת, ניהול המשא ומתן בנוגע לאבטחה ייכשל, והלקוחות לא יוכלו לגשת למשאבי רשת.

כאשר DNS אינו מאפשר IPSec

כדי לציין שם DNS של מארח במפרט IP Filter List (במקום את כתובת ה-IP), במידה ושרתי ה-DNS אינם מאפשרים IPSec, נדרשת הגדרה מיוחדת במדיניות. אחרת, IPSec לא יצליח לתרגם כהלכה את שם מארח ה-DNS לכתובת IP חוקית. ההגדרה מורכבת ממפרט מסנן המסתיר את התעבורה שבין המארח לשרת ה-DNS מפני IPSec הדורש זאת.

הוסף מפרט מסנן למדיניות היישום, וכלל.

➢ **בכרטיסיה Addressing שבתיבת דו-שיח IP Filter List**

1. קבע את הכתובת Source ל- My IP address.
2. קבע את הכתובת Destination ככתובת ה-IP של שרת ה-DNS.
3. סמן את Mirrored כדי שייצור באופן אוטומטי את מפרט מסנן היציאה.

➢ **בכרטיסיה Protocol שבתיבת דו-שיח IP Filter List**

1. בתיבות From this port ו- To this port קבע את הערך 53 (זוהי היציאה המקובלת המשמשת את רוב שרתי DNS להתקשרות; קבע ערך זה כך שיתאים למספר היציאה שהוגדרה בשירות ה-DNS לשימוש התעבורה).

בנוסף, מדיניות ניהול המשא ומתן עבור כלל זה חייבת להיות מוגדרת כ- Do not allow secure communication: No security methods should be configured. דבר זה יבטיח שתעבורת DNS לעולם לא תהיה מאובטחת אמצעות IPSec.

מאפייני TCP/IP

אם מחשב החבר ב-domain מנותק מה-domain שלו, עותק של מאפייני IPSec של ה-domain יאוחזר מרישום המערכת (Registry) של המחשב. אם המחשב אינו חבר ב-domain, תאוחסן מדיניות IPSec מקומית ברישום המערכת במחשב. מאפייני TCP/IP מאפשרים למחשב שאינו חבר ב-domain להשתמש תמיד ב-IPSec, להשתמש ב-IPSec רק בעת הצורך, או שלא להשתמש ב-IPSec כלל.

הערה אם המחשב מחובר ל-domain, מאפיינים אלה לא יהיו ניתנים להגדרה.

תרגול: בניית מדיניות IPSec מותאמת אישית

מספר מדיניות הוגדרו מראש, כדי לאפשר לך לבחון ולחקור את התנהגותן והגדרותיהן. אבל, ברוב המקרים בהם תיישם את IPSec תידרש ליצור מדיניות מותאמת אישית. תרגול זה ילמד אותך לבנות מדיניות IPSec משלך. עליך לבצע תרגול זה בשני המחשבים.

➢ **כדי ליצור מדיניות IPSec משלך**

1. לחץ Start, הצבע Programs, הצבע על Administrative Tools והפעל את יישום ה-Snap-In של MMC, Local Security Policy.

2. בחלונית השמאלית לחץ לחיצה ימנית על IP Security Policy On Local Machine.
3. מתפריט הקיצור בחר Create IP Security Policy.
4. כאשר מופיע האשף, לחץ Next כדי להמשיך.
5. הקלד עבור המדיניות את השם Two Computer Policy, ולחץ Next.
6. במסך Requests For Secure Connection השאר את ברירות המחדל כפי שהן (השאר את הסימון בתיבת הסימון Default Response Rule), ולחץ NEXT.
7. השאר את ברירת המחדל Kerberos Authentication של כלל התגובה כפי שהיא, ולחץ NEXT.
8. ודא שתיבת הסימון Edit Properties אכן מסומנת.
9. לחץ על FINISH כדי לסיים את ההגדרה הראשונית.
10. כעת מופיעה תיבת דו-שיח Properties. **אל תסגור אותה!**

בנקודה זו, עדיין לא הגדרת את הכלל המותאם אישית. הוגדרו רק מאפייני כלל תגובת ברירת המחדל (Default Response Rule Properties).

מהי מטרת כלל תגובת ברירת המחדל?

ליתרת תרגול זה לא תשתמש באשף Add כאשר תגדיר מדיניות IPSec. במקום זאת, תגדיר מדיניות באופן ידני על ידי ניווט בין תיבות דו-שיח וכרטיסיות מאפיינים.

➢ כדי להוסיף כלל חדש

1. בתחתית תיבת דו-שיח Properties, בטל את הסימון ליד תיבת הסימון Use Add Wizard.
2. בכרטיסיה Rules במסך Properties לחץ Add.
3. מופיע המסך New Rule Properties.

כעת תגדיר מסננים בין המחשב שלך והמחשב השני שלך. תצטרך להגדיר מסנן יציאה תוך ציון כתובת ה-IP שלך ככתובת המקור ואת המחשב השני שלך ככתובת היעד. אז, יגדיר תהליך השיקוף באופן אוטומטי מסנן כניסה, המציין את הכתובת של המחשב השני שלך ככתובת המקור, ואת המחשב שלך ככתובת היעד.

➢ כדי להוסיף מסנן חדש

1. לחץ Add. מופיע IP Filter List.
2. בתיבה Name הקלד את השם Host A-Host B Filter עבור מסנן זה.
3. בטל את הסימון ליד תיבת הסימון Use Add Wizard.
4. בכרטיסיה IP Filter List, לחץ Add.
5. התיבה Filter Properties מופיעה.
6. שנה את Source Address לכתובת IP מסוימת.

7. הוסף את כתובת ה-IP שלך (w.x.y.z).

8. שנה את Destination Address לכתובת IP מסוימת.

9. הוסף את כתובת ה-IP של המחשב השני שלך (w.x.y.z).

10. לחץ OK. ודא שהמסנן שלך נוסף בתיבה Filters שבתיבת דו-שיח IP Filter List.

11. לחץ Close.

12. בכרטיסיה IP Filter List, הפעל את המסנן שלך על ידי לחיצה על לחצן האפשרויות שליד רשימת המסננים שזה עתה הוספת.

בהליך קודם הגדרת מסנני כניסה ויציאה להשוואה בין מנות תקשורת תואמות. בהליך הבא תגדיר את את הפעולות בהן יש לנקוט על מנות מסוננות.

➢ כדי לציין פעולה של מסנן

1. בחר בכרטיסיה Filter Action ובטל את הסימון ליד תיבת הסימון Use Add Wizard.

2. לחץ Add כדי ליצור פעולת מסנן.

3. בכרטיסיה Security Method ודא שנבחרה אפשרות Negotiate Security.

4. ודא שאפשרות Allow unsecured communication with non IPSec aware computer אינה נבחרת.

5. לחץ Add כדי לבחור שיטת אבטחה.

6. בחר Medium (AH), ולחץ OK.

7. לחץ OK כדי לסגור את תיבת דו-שיח New Filter Action Properties.

8. לחץ על לחצן האפשרויות שליד המסנן שזה עתה יצרת, כדי להפעיל אותו.

בהליך זה תציין כיצד שני המחשבים יתנו אמון (Trust) אחד בשני, על ידי ציון שיטת האימות שתשמש בעת הניסיון להקמת SA. בהליך זה תעשה שימוש במפתח משותף מראש (Preshared Key). זוהי מילה או משפט אותם חייבים שני המחשבים להכיר כדי שיוכלו לתת אמון אחד בשני. שני צידי התקשרות IPSec חייבים להיות מודעים לערך זה. ערך זה אינו משמש להצפנת נתוני היישום. להיפך מכך, הוא משמש רק בעת המשא ומתן לקביעה האם שני המחשבים יכולים לסמוך האחד על האחר.

➢ כדי לקבוע שיטת אימות

1. בחר בכרטיסיה Authentication Method.

2. לחץ Add.

3. לחץ על לחצן האפשרויות Pre-Shared Key.

4. בתיבת הטקסט, הקלד את משפט המפתח או סיסמה, ולחץ OK.

5. מהרשימה, סמן את Pre-Shared Key ולחץ על לחצן Move Up, כך שהוא יופיע ראשון ברשימה.

➢ כדי לוודא הגדרות תעלה

1. בחר בכרטיסיה Tunnel Settings.
2. ודא שאפשרות This rule does not specify an IPSec tunnel נבחרה.

➢ כדי לוודא הגדרות סוג חיבור

1. בחר בכרטיסיה Connection Type.
2. ודא שהאפשרות All network connections נבחרה.

➢ כדי להשלים את יצירת הכלל

1. לחץ Close, כדי לחזור לתיבת דו-שיח Policy Properties, והשלם את יצירת הכלל.
2. ודא שנבחרה אפשרות This new rule מהרשימה.
3. סגור את תיבת דו-שיח Policy Properties.

➢ כדי להפעיל את המדיניות החדשה

1. בחלונית הימנית של MMC, לחץ לחיצה ימנית על המדיניות Two Computer Policy שיצרת.
2. מתפריט הקיצור בחר Assign.
3. העמודה Policy Assigned צריכה להציג כעת את הערך Yes.

➢ כדי לבחון את IPSec

1. אפשר (Enable) את המדיניות במחשב שלך ובמחשב השני.
2. בצע PING למחשב השני.
3. פעולת PING הראשונה לאחר אפשור המדיניות בדרך כלל תיכשל, בשל הזמן שאורך ניהול המשא ומתן לגבי המדיניות.
4. כאשר בשני המחשבים פועלות מדיניות תואמות, פעולות PING בעתיד יצליחו.
5. לחילופין, הפעל ובטל את המדיניות במחשב שלך ובמחשב האחר, כדי לראות את השפעתן של הגדרות מדיניות שאינן תואמות.

סיכום שיעור

קל מאוד להתאים את IPSec לצרכיך האישיים באמצעות מדיניות וכללים. בשיעור זה למדנו כיצד לאבטח את הרשת שלנו תוך שימוש בשיטות שונות, וכיצד יש להתחשב בדברים כגון שרתי Proxy, NAT, SNMP, DHCP, DNS, WINS ו- **D**omain **C**ontrollers (DCs).

שיעור 4: ניטור IPSec

כדי לראות כיצד נעשה שימוש במדיניות וכללי IPSec שלך ברשת, ייתכן שתרצה לנטר את IPSec. בשיעור זה תשתמש במספר כלים לשם כך. תתמקד בכלי ניטור IPSec כגון IPSECMON.EXE, Event Viewer, Performance Monitor ו- Network Monitor. כלים אלה יסייעו לך לשמר סביבת רשת מאובטחת ועשירת IPSec.

לאחר שיעור זה, תוכל

- לאתר ולטפל בתקלות באמצעות IPSECMON.EXE.
- לאתר ולטפל בתקלות באמצעות Event Viewer.
- לאתר ולטפל בתקלות באמצעות Network Monitor.
- לתאר איתור וטיפול בתקלות באמצעות קבצי היומן IPSECPA.LOG ו- OAKLEY.LOG.

זמן לימוד משוער: 30 דקות

כלי ניהול ואיתור תקלות של IPSec

Windows 2000 מספקת כלים בהם תוכל להיעזר לניהול ולאיתור תקלות IPSec. סעיף זה מספק סקירה של כלים אלה.

כלי ניהול

- יישום Snap-In בשם IP Security Policy Management יוצר ועורך מדיניות (ניתן להשתמש גם ב- Group Policy Editor).
- כלי IP Security Management גם הוא נמצא כברירת מחדל בנתיב Start, Programs, Administrative Tools.

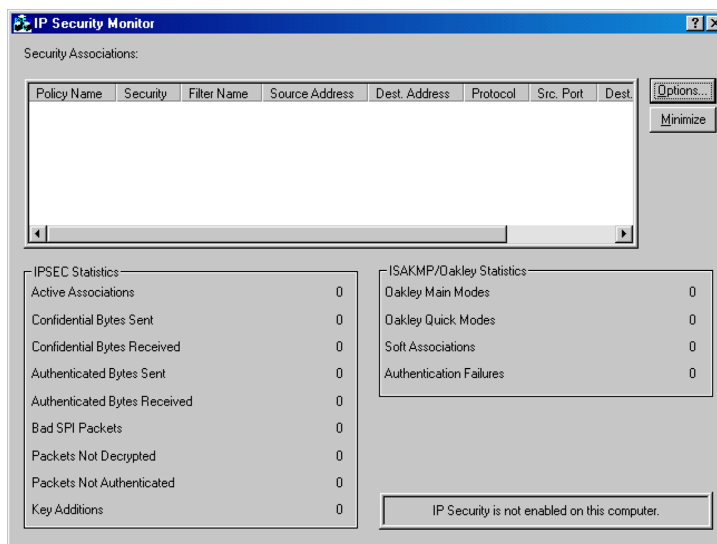
כלי ניטור ואיתור תקלות

IP Security Monitor (הקובץ IPSECMON.EXE), אותו ניתן לראות בתרשים 5.13, מופעל ממנחה שורת הפקודה (Command Prompt). כלי זה מנטר Sas, שגיאות משא ומתן, תוספות מפתח (Rekey) וסטטיסטיקות אבטחת IP אחרות.

סטטיסטיקות IPSec

IP Security Monitor מסוגל למדוד את סטטיסטיקות IPSec הבאות:

- **Active Associations.** מונה פשוט של SAs.
- **Confidential Bytes Sent/Recvived.** סך כל הבתים (Bytes) שנשלחו / התקבלו באמצעות פרוטוקול ESP.
- **Authenticated Bytes Sent/Recvived.** סך כל הבתים שנשלחו / התקבלו באמצעות פרוטוקול AH.



תרשים 5.13 IP Security Monitor

- **Bad SPI Packets.** מספר הכולל של מנות שגיאה לגבי SPI. כפי שנדון קודם לכן, SPI משמש להשוואת מנות נכנסות מול SAs. אם SPI פגום יכול הדבר להצביע על כך שתוקפו של SA נכנס פג, אך הגיעה מנה לה SPI ישן. מספר זה יגדל במקרה והפרשי הזמן בין תוספות מפתחות (Rekeys) קצרים, וקיים מספר גדול של SAs. מכיון שתוקפו של SA מועד לפוג, אין הדבר מצביע בהכרח על כך ש-IPSec אינו ממלא את תפקידו.
- **Packets Not Decrypted.** מספר הכולל של מנות שהצפנתן נכשלה. כפי שהדבר עם מנות SPI פגומות, כשל כגון זה מצביע על כך שהגיעה מנה שפג תוקפו של ה-SA שלה. אם פג תוקף ה-SA, פג גם תוקפו של מפתח השיח (Session Key) המשמש לפענוח המנה. אין הדבר מצביע בהכרח על כך ש-IPSec אינו ממלא את תפקידו.
- **Packets Not Authenticated.** בדומה לשתי הנקודות הקודמות, זהו מספר הכולל של מנות המכילות נתונים שלא ניתן היה לאמת אותם. הסיבה השכיחה ביותר היא שפג תוקפו של ה-SA.
- **Key Additions.** מספר הכולל של המפתחות אותם שלח ISAKMP למנהל התקן IPSec. ערך זה מציין את המספר הכולל של משא ומתן מסוג Phase 2 שהושלמו בהצלחה.

סטטיסטיקות ISAKMP/Oakley

IP Security Monitor מסוגל למדוד את סטטיסטיקות ISAKMP/Oakley הבאות:

- **Oakley Main Modes.** מספר כולל של SA מוצלחים של ISAKMP שנוצרו במהלך Phase 1 של משא ומתן.
- **Oakley Quick Modes.** מספר כולל של SA מוצלחים של IPSec שנוצרו במהלך Phase 2 של משא ומתן. מכיון שייתכן שתוקפם של SAs אלא עשוי לפוג בקצבים שונים, מספר זה עשוי שלא להיות תואם למספר Main Modes.

- **Soft Associations.** מספרם הכולל של משא ומתן Phase 2 שתוצאותיהם היו הסכמה על שימוש בטקסט נקי. בדרך כלל יהיה זה מספר השיוכים שנוצרו עם מחשבים שאינם מודעי-IPSec (non-IPSec-Aware Computers).
- **Authentication Failures.** מספרם הכולל של אימותי זהות שנכשלו (Kerberos, אישורי משתמש, סיסמאות שהוגדרו באופן ידני). אין הדבר דומה לסטטיסטיקה Packets Not Authenticated (אימות הודעות באמצעות Hash).

הערה כדי לאפס את מוני הסטטיסטיקה ב- IP Security Manager, הפעל מחדש את IP Security Policy Agent.

כלי Performance monitor כולל גם אובייקטי IPSec ומונים הניתנים לבדיקה. אירועים אלה יכולים גם להירשם ולהיות מנותחים בשלב מאוחר יותר באמצעות Event Viewer :

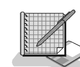
- אירועים של סוכן המדיניות ושל מנהל התקן IPSec, ביומן המערכת (System Log).
- אירועי Oakley, ביומן היישומים (Application Log).
- אירועי ISAKMP (פרטי SA) ביומן האבטחה (Security Log), במידה ומאופשרת ביקורת כניסה למערכת, (Logon Auditing).

שימוש ב- Network Monitor

Network Monitor Version הוא כלי יעיל לאיתור וטיפול בתקלות IPSec. גם הגירסה המצומצמת, המצורפת למערכת ההפעלה Windows 2000 Server, וגם הגירסה המלאה, המצורפת למוצר Microsoft System Management Server גירסה 2, מציגות מנתחים (Parsers) עבור ISAKMP, AH ו-ESP. Network Monitor לוכד את כל הנתונים המועברים בממשקי הרשת בכל רגע נתון.

גירסה 2 של Network Monitor מכילה מנתח למנות IPSec. אם IPSec מצפין את המנות יהיה תוכנן בלתי ניתן לצפייה, אבל המנה עצמה כן תהיה ניתנת לצפייה. אם נעשה שימוש באימות בלבד, כל המנה, כולל התוכן שלה, יהיו ניתנים לצפייה. ESP יוצג כפרוטוקול IP מספר 50 (דצימלי) ו-AH יוצג כמספר 51 (דצימלי). ISAKMP/Oakley יוצג כיציאת UDP מספר 500 (דצימלי).

הערה נתוני ESP עצמם לא יהיו קריאים בשל ההצפנה.



תרגול: שימוש ב- Network Monitor לצפייה בתעבורת טקסט נקי

תוך שימוש בכלי זה, תלכוד ותצפה בנתונים הנשלחים בחיווט הרשת בין המחשב שלך והמחשב האחר. גירסה 2.0 של Network Monitor מכילה מנתח עבור מנות IPSec ו- ISAKMP. Network Monitor מקבל את המנות אחרי IPSec, כך שאם IPSec מצפין את המנה לא ניתן יהיה לצפות בתוכן שלה.

הערה בצע את כל ההליך בשני המחשבים. תרגיל זה יתבצע בכל מחשב, אחד אחרי השני.

➢ כדי לצפות במנות שלמות של IPSec (בפורמט AH)

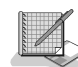
1. הפעל את Network Monitor וקבע את רשת הלכידה לכתובת בקרת הגישה למדיה (Media Access Control Address) של כרטיס הרשת המחובר למחשב האחר.

הערה תוכל להפעיל את פקודה ipconfig עם הפרמטר all/ כדי לאתר את כתובת בקרת הגישה למדיה של כרטיס הרשת שלך.

2. בממשק MMC - Local Security Settings, שייך (Assign) את המדיניות Two Copmuter Policy (זו שיצרת בתרגול של שיעור 3).
3. התחל את לכידת המנות באמצעות Network Monitor.
4. הפעל את תוכנית השירות IPSECMON.EXE.
5. בצע PING לכתובת IP של המחשב השני שלך.
6. ייתכן שתיאלץ לבצע שלב זה פעם נוספת, מפני של-PING יש פסק-זמן קצר מאוד ונדרש זמן מה לשיוך IPSec בין שני המחשבים.
7. עצור את הלכידה וצפה ברשומות המעקב של Network Monitor.
8. הבט בחלון של ipsecmon.
9. לחץ לחיצה כפולה על מנת **I**nternet **C**ontrol **M**essage **P**rotocol (ICMP) הראשונה.
10. שים לב שאתה רואה שורות המציינות כותרות עבור מסגרות, Ethernet, IP ו-AH.
11. בחלונית Details הרחב את הרשומה IP.
12. רשום את מספר פרוטוקול IP.

גלול לתחתית פרטי IP ולחץ על המקום בו מופיע IP Data: Number of data bytes remaining = 64 (0x0040). שים לב שתוכן IP מופיע בטקסט נקי. הנתונים ב-PING הם abcdefghi...

IPSec יוצר מהכותרות IP, ICMP ו-Data ערך ICV של המסגרת. בעשותו כן הוא מונע ממישהו אחר מללכוד את הנתונים, לשנותם ולהמשיך ולשלוח את הנתונים המטופלים. אם תביט בחלונית Hex, תוכל עדיין לראות את 32 התווים שנשלחו על ידי PING. על ידי הגדרת שיטת אבטחה AH אנו מבטיחים אימות, אך איננו מצפינים את הנתונים במנה. AH רק מוודא שנתוני המנה, כמו גם רוב חלקי כותרת ה-IP, כגון כתובות IP של המקור ושל היעד, לא ישונו. כעת, נביט במנות תוך שימוש בשיטת האבטחה ESP אשר תצפין את חלק הנתונים של מנת IP.



תרגול: שימוש ב- Network Monitor לצפייה בתעבורת מוצפנת

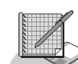
בתרגול זה תשתמש ב- Network Monitor כדי לקבוע הצפנת ESP ולצפות במנות מוצפנות.

➢ **כדי לקבוע הצפנת ESP**

1. בטל (Unassign) את המדיניות Two Computer Policy.
2. ערוך את המדיניות Two Computer Policy על ידי לחיצה ימנית עליה ומתפריט הקיצור בחירה באפשרות Properties.
3. בחר בכרטיסיה Filter Action.
4. ערוך את New Filter Action הפעיל.
5. לחץ Edit כדי לשנות את Security Method.
6. שנה את הערך Medium לערך (High (ESP.
7. סגור את כל תיבות הדו-שיח.
8. שייך את המדיניות Two Computer Policy.

➢ **כדי לצפות במנות IPSec מוצפנות ESP**

1. התחל את לכידת המנות באמצעות Network Monitor.
2. הפעל את תוכנית השירות ipsecmon.
3. בצע PING לכתובת ה-IP של המחשב האחר.
4. בצע PING לכתובת IP של המחשב השני שלך.
5. ייתכן שתיאלץ לבצע שלב זה פעם נוספת, מפני של-PING יש פסק-זמן קצר מאוד ונדרש זמן מה לשיוך IPSec בין שני המחשבים.
6. עצור וסקור את רשומות המעקב של Network Monitor.
7. לחץ לחיצה כפולה על מסגרת ESP הראשונה.
8. הפעם אתה אמור לראות ארבע רשומות בחלונית Details: Frame, Ethernet, IP ו-ESP. IPSec יצר Hash מהשדות ICMP ו-Data של המסגרת.
9. הרחב את הקטע IP ורשום לפניך את פרוטוקול IP.
10. גלול לתחתית פרטי IP ולחץ לחיצה כפולה על המקום בו מופיע IP: Data: Number of data bytes remaining = 76 (0x004C). הבט בחלונית Hex; תראה שהנתונים הוצפנו.



תרגול: שימוש בעזרי אבחון

בתרגול זה תשתמש בכלי האבחון IPSec Monitor כדי לוודא ש-IPSec פעיל וכדי לצפות ב- SAs פעילים.

שימוש ב- IPSec Monitor

Windows 2000 Server כוללת גם כלי ניטור עבור IPSec, הנקרא IPSecmon. הפעל כלי זה כדי לראות שיוכי אבטחה פעילים, קשיחים ("Hard") או רכים ("Soft"), במכונה המקומית או במכונה מרוחקת. כלי זה אינו מציג SAs שנכשלו, או מסננים אחרים.

לחץ Start, בחר Run ובתיבת הטקסט Open הקלד את הפקודה:

ipsecmon [machine name]

עבור כל SA קשה או רך תראה שורה אחת בתיבה הלבנה. העמודה שמשמאל, כותרתה Policy Name, מכילה את שם המדיניות ששויכה ונאכפה על מחשב זה. העמודה Negotiation Policy היא שיטת האבטחה המעשית שעליה הוסכם בעת המשא ומתן. נעשה ניסיון לתרגם את כתובות ה-IP של המקור והיעד לשמות DNS.

יש לשים לב למספר סטטיסטיקות גלובליות המצטברות מאז שהמחשב אותחל לאחרונה:

- SAs מוצלחים של IPSec יגרמו בסופו של דבר ל- ISAKMP/Oakley Main Mode אחד ול- Quick Mode אחד. פעילויות חידוש מפתחות יוצגו בדרך כלל כ- Quick Mode נוספים.
- מספרם הכולל של בתים סודיים (ESP) או של בתים מאומתים (ESP ו-AH) שנשלחו או התקבלו עבור כל SAs הקשיחים מוצג משמאל. מכיון ש-ESP מספק גם סודיות וגם אימות, שני המונים מקודמים. מכיון ש-AH מספק אימות, אבל לא סודיות, מקודם רק המונה Authenticated-Byte-Sent.
- מספרם הכולל של שיוכים "רכים" מוצג מימין.

כדי לבדוק אם IPSec פעיל ולצפות ב- SAs פעילים

1. פתח את לוח הבקרה וממנו את Network and Dial-up Connections.
2. לחץ לחיצה ימנית על Local Area Connection, ומתפריט הקיצור בחר Properties.
3. סמן את הפרוטוקול Internet Protocol (TCP/IP), ולחץ Properties.
4. לחץ Advanced.
5. בחר בכרטיסיה Options, בחר IP Security, ולחץ Properties.

אם המחשב משתמש במדיניות מקומית, יוצג שם המדיניות המקומית תחת Use this IP Security policy. אם אתה משתמש במדיניות המשויכת באמצעות מנגנון מדיניות קבוצתית ב- Active Directory, תיבת הדו-שיח תהיה מעומעמת ויוצג בה שם המדיניות המשויכת.

סיכום שיעור

הראנו כיצד לצפות במדיניות ובכללי IPSec המשמשים ברשת. בשיעור זה השתמשת במספר כלים כדי לעשות זאת. התמקדת בכלי ניטור IPSec כגון IPSECMON.EXE ו- Network Monitor. כלים אלה יסייעו לך לנטר, לאתר ולטפל בבעיות תקשורת הקשורות ב-IPSec ברשת שלך.

שאלות סיכום

השאלות הבאות נועדו לחזק את הנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות על שאלה, עיין בשיעור המתאים ונסה את השאלה שנית. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואחר כך בעברית.

Answering the following questions will reinforce key information presented in this chapter. If you are unable to answer a question, review the appropriate lesson and then try the question again. Answers to the questions can be found in Appendix A, "Questions and Answers".

1. IPSec is defined by what standards group?
2. Define the difference between secret and public key cryptography.
3. ISAKMP/Oakley provides what functionality?
4. What are rules comprised of?
5. When would a public key certificate be used?
6. What is an IP filter used for?

1. IPSec מוגדר על ידי איזו קבוצה תקנית?
2. הגדר את ההבדלים שבין הצפנת מפתח סודי להצפנת מפתח ציבורי.
3. איזו פונקציונליות מספק ISAKMP/Oakley?
4. ממה מורכבים כללים?
5. מתי יש להשתמש באישור מפתח ציבורי?
6. למה משמש מסנן IP?

פרק 6

הסדרת שמות
מארחי רשת (Host)

אודות פרק זה

בעת השימוש ברשת, הן לקוחות והן שרתים ברשת חייבים להסדיר (לתרגם) את השמות הידידותיים של המארחים לכתובות IP. בפרק זה תלמד כיצד פרוטוקול TCP/IP מסדיר (Resolves) שמות מארחים. ידע זה חשוב כשאתה מתכנן את הרשת שלך ומתכנן כיצד יוסדרו השמות וכתובות ה-IP. אפשרויות מתקדמות של הסדרה, כגון: DNS (**D**omain **N**ame **S**ystem) או WINS (**W**indows **I**nterface **N**ame **S**ervice), יתוארו בהמשך הפרק.

לפני שתתחיל

להשלמת פרק זה עליך:

- ❖ להשלים את קריאת פרק 2.

שיעור 1: סכמת מתן השמות ב-TCP/IP

כאשר מחשבים מתקשרים ומחליפים ביניהם נתונים ברשת TCP/IP, הם משתמשים בכתובות IP מסוימות שהוקצו להם, ואשר משויכות למארח המסוים שלהם. לדוגמה, הרבה יותר קל למשתמש לזכור את הכתובת www.microsoft.com, מאשר את כתובת IP המסוימת המשויכת לאתר אינטרנט זה. למרות שמארח TCP/IP דורש כתובת IP לצורך ההתקשרות, ניתן להתייחס למארחים בשמות, במקום בכתובת IP. מכיון ששמות מבוססי טקסט יכולים לשמש כתחליף לכתובות IP, חייב להיות מנגנון כלשהו שישייך את השמות הללו לצוות IP המתאים. דבר זה מבטיח את ייחודיות השם ואת שיוכו לכתובת IP המתאימה.

לאחר שיעור זה, תוכל

- להסביר את סכמות מתן השמות השונות בהן משתמשים מארחים.

זמן לימוד משוער: 10 דקות

סכמות מתן שמות של Windows 2000

Windows 2000 מספקת מספר סוגים שונים של הסדרת שמות, כולל DNS, WINS, הסדרת שמות בשידור רחב (Broadcast Name Resolution) והסדרת שמות באמצעות הקובץ HOSTS או הקובץ LMHOSTS. Windows 2000 משתמש בשיטה שונה להסדרת השמות מזו שמשתמשים מארחים אחרים, כדוגמת מארחי UNIX. ניתן לשייך שם למארח Windows 2000, אך שם זה משמש רק בעת העבודה עם יישומי TCP/IP. מארחי UNIX דורשים רק כתובת IP. השימוש בשם מארח או שם Domain לצורך ההתקשרות הוא בגדר אפשרות.

לפני שניתן לבצע התקשרות, יש לקבוע כתובת IP לכל מארח TCP/IP. אבל, סכמת מתן השמות (Naming Scheme) משפיעה על אופן ההתייחסות למארח. לדוגמה:

❖ כדי לבצע את הפקודה NET USE בין שני מחשבי Windows 2000 עומדות בפני המשתמש מספר אפשרויות לגבי אופן ציון שם המחשב.

כל אחת משלוש האפשרויות הבאות תעבוד:

```
net use x: \\netbios_name\share
net use x: \\10.1.3.74\share
net use x: \\host.domain.com\share
```

שם NetBIOS או שם המארח חייבים להיות מתורגמים לכתובת IP לפני ש-ARP (**A**ddress **R**esolution **P**rotocol) יכול להסדיר את כתובת ה-IP לכתובת חומרה. אם נעשה שימוש בכתובת IP, לא נדרשת הסדרה מסוג כלשהו.

- ❖ כדי להתייחס למארח UNIX המפעיל TCP/IP, צריך המשתמש לציין כתובת IP או שם מארח. אם נעשה שימוש בשם מארח, השם מתורגם (מוסדר) לכתובת IP. אם נעשה שימוש בכתובת IP לא נדרשת הסדרה כלשהי וכתובת ה-IP מתורגמת לכתובת החומרה.

סיכום שיעור

ניתן להתייחס הן למארחי Windows 2000 והן למארחי UNIX באמצעות כתובת ה-IP שלהם או באמצעות שם המארח שלהם. מערכת ההפעלה Windows 2000 ומערכות הפעלה לרשת אחרות מבית Microsoft מאפשרות מיעון על פי כתובת NetBIOS.

שיעור 2: שמות Hosts

שם מארח מפשט את האופן בו מתייחסים אל המארח, מפני שלאדם הממוצע קל יותר לזכור שם מאשר כתובות IP. השימוש בשמות מארחים הוא לכל אורך ורוחב סביבת TCP/IP. שיעור זה מתאר כיצד פועלת הסדרת שם מארח (Host Name Resolution).

לאחר שיעור זה, תוכל

- להסביר כיצד מסדיר הקובץ HOSTS שם מארח לכתובת IP.
- להסביר כיצד מוסדר שם מארח לכתובת IP תוך שימוש בשרת DNS ושיטות נתמכות-Microsoft.

זמן לימוד משוער: 20 דקות

מהם שמות מארחים?

שם מארח (Host Name) הוא כינוי המשוייך לרכיב IP (IP Node) שנועד לצורך זיהויו כמארח TCP/IP. שם המארח יכול לכלול עד 255 תווים, כולל כל התווים האלפאנומריים והתווים מקף (-) ונקודה (.). ניתן לשייך מספר שמות מארח לאותו מארח. במחשבים הפועלים בסביבת Windows 2000 לא חייב שם המארח להיות זהה לשם המחשב ב-Windows 2000.

יישומי שקעי Windows (WinSock, Windows Sockets Applications), כגון: Internet Explorer ותוכנית השירות של FTP (**F**ile **T**ransfer **P**rotocol), יכולים להשתמש באחד מהערכים כיעד ההתחברות: כתובת ה-IP או שם המארח. כאשר מצוינת כתובת ה-IP אין צורך בהסדרת שמות (Name Resolution). כאשר מצוין שם המארח חייב שם המארח להיות מוסדר (מתורגם) לכתובת IP, לפני שניתן יהיה לבצע התקשרות מבוססת IP עם היעד.

לשמות מארח יכולים להיות מבנים שונים. שני המבנים השכיחים ביותר הם שם כינוי (Nickname) ושם domain (Domain Name). שם כינוי הוא כינוי לכתובת IP בו יכולים משתמשים בודדים להשתמש ואותה ניתן לשייך. שם domain הוא שם מובנה המחוייב במוסכמות האינטרנט.

מטרות שם מארח

שם מארח הוא כינוי שהוקצה למחשב על ידי מנהל המערכת (Administrator), כדי לזהות מארח TCP/IP. שם המארח אינו חייב להיות זהה לשם NetBIOS של המחשב, ויכול לכלול עד 255 תווים אלפאנומריים. ניתן להקצות מספר שמות מארח לאותו מארח.

שם מארח מפשט את אופן ההתייחסות של המשתמש למארחי TCP/IP אחרים. קל יותר לזכור שמות מארחים מאשר כתובות IP. בעצם, תוכל להשתמש בשם מארח גם בעת ביצוע הפקודה PING, או בעת השימוש ביישומי TCP/IP אחרים.

שם מארח מקביל תמיד לכתובת IP המאוחסנת בקובץ HOSTS, או במסד הנתונים שבשרת DNS. לקוחות Windows יכולים לתרגם שמות מארחים ושמות NetBIOS במקרים רבים, תוך מתן אפשרות לשרת WINS לבצע את הסדרת השמות לשם המארח.

תוכנית השירות hostname תציג את שם המארח שהוקצה למערכת שלך. כברירת מחדל, שם המארח הוא שם המחשב שלך המפעיל את Windows 2000.

הסדרת שם מארח

הסדרת שם מארח (Host Name Resolution) הוא התהליך של מיפוי שם מארח לכתובת IP. לפני שניתן להסדיר כתובת IP לכתובת חומרה (Hardware Address), חייב שם המארח להיות מוסדר לכתובת IP.

Windows 2000 יכולה להסדיר שמות מארחים תוך שימוש במספר שיטות, וביניהן:

- **הסדרת שמות NetBIOS.** NetBIOS מגדיר ממשק ברמת-שיח (Session-Level Interface) ופרוטוקול ניהול/תעבורת נתונים של שיח (Session Management/Data Transfer Protocol). כדי להתממשק עם מארחי NetBIOS משתמש NetBIOS ברישום שמות (Name Registration), שחרור שמות (Name Release) וגילוי שמות (Name Discovery). הסדרת שמות NetBIOS (NetBIOS Name Resolution) הוא תהליך מיפוי שם NetBIOS של המחשב לכתובת IP. קיימות מספר שיטות זמינות להסדרת שמות כזו, כל אחת מהן מסתמכת על תצורת הרשת שלך. השיטות הן הכנסה למטמון של שם NetBIOS (NetBIOS Name Cache), שרת שמות NetBIOS (NetBIOS Name Server), שידור רחב מקומי (Local Broadcast), קובץ LMHOSTS, קובץ HOSTS ו-DNS.
- **הסדרת שמות באמצעות הקובץ HOSTS.** הקובץ HOSTS הוא קובץ טקסט המאוחסן באופן מקומי במערכת, ואשר מכיל שמות מארחים ואת כתובת ה-IP המשויכים להם. בשיעור הבא נדון בהרחבה בקובץ HOSTS.
- **הסדרת שמות באמצעות שרת DNS.** שרת DNS הוא מסד נתונים מקוון מרכזי המשמש ברשתות IP להסדרת שמות Domains מסוג FQDN (**F**ully **Q**ualified **D**omain **N**ame) ושמות מארחים אחרים, לכתובות IP. Windows 2000 יכולה להשתמש בשרת DNS ולספק שירותי שרת DNS. נושא ה-DNS מוסבר בהרחבה בפרק 7.

פרוטוקול TCP/IP יכול להיעזר בכל אחת מהשיטות הנזכרות בטבלה 6.1 ובטבלה 6.2 כדי להסדיר שמות מארחים. השיטות בהן יכולה Windows 2000 להשתמש להסדרת שמות מארחים ניתנות להגדרה.

טבלה 6.1 שיטות תקניות להסדרת שמות מארחים

שיטת הסדרה	תיאור
שם מארח מקומי	שם המארח המוגדר למחשב. שם זה מושווה לשם מארח היעד
הקובץ HOSTS	קובץ טקסט מקומי בפורמט תואם לקובץ בתקן 4.3 Berkeley Software Distribution UNIX/Etc/HOSTS. קובץ זה ממפה שמות מארחים לכתובות IP. משמש בדרך כלל להסדרת שמות עבור יישומי TCP/IP.
שרת DNS	שרת המתחזק מסד נתונים של מיפוי כתובות IP לשמות מארחים.

טבלה 6.2 שיטות Microsoft להסדרת שמות מארחים

שיטת הסדרה	**תיאור**
שרת שמות NetBIOS	שרת המיושם בהתאם ל- RFC 1001 ו- RFC 1002 (RFC, Request For Comments) להספקת הסדרת שמות NetBIOS של מחשבים. יישום Microsoft להסדרה זו הוא WINS.
Local Broadcast	Broadcast ברשת המקומית עבור כתובת IP של שם NetBIOS היעד.
הקובץ LMHOSTS	קובץ טקסט מקומי הממפה כתובות IP לשמות NetBIOS של מחשבים מארחים מבוססי-Windows.

הסדרת שמות NetBIOS

שם NetBIOS הוא כתובת ייחודית בת 16 סיביות המשמשת לזיהוי משאב NetBIOS ברשת. תהליך הסדרת שם NetBIOS ממיר את שם NetBIOS לכתובת IP. דוגמה לתהליך המשתמש בשמות NetBIOS ניתן למצוא בשירות File and Print Services for Microsoft Networks במחשב הפועל בסביבת Windows 2000. כאשר המחשב מאותחל, השירות רושם File and Print Services for Microsoft Networks שם NetBIOS ייחודי, המבוסס על שם המחשב שלך. מחשבים המפעילים את TCP/IP יכולים להשתמש בהסדרת שמות באמצעות Local Broadcast, שהוא מצב הפעלה NetBIOS-over-TCP/IP. שיטה זו סומכת על מחשב המבצע Broadcast ברמת IP, כדי לרשום את שמו על ידי הכרזה (Announcement) עליו ברשת. כל מחשב באיזור השידור הרחב אחראי על מניעת רישום כפול של שמות ועל הגבה לשאילתות המיועדות לשמו הרשום.

הסדרת שמות באמצעות הקובץ HOSTS

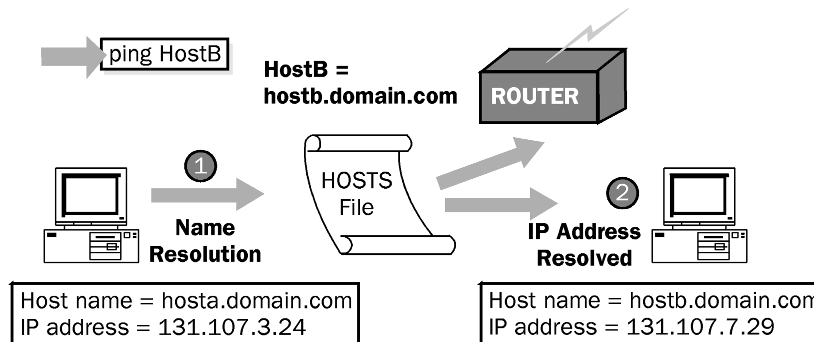
כפי שניתן לראות בתרשים 6.1, תהליך הסדרת השמות באמצעות הקובץ HOSTS הוא כזה:

1. הסדרת השמות מתחילה כאשר משתמש קורא ליישום מבוסס-WinSock באמצעות שם מארח, ולא כתובת IP.
2. Windows 2000 בודקת כדי לראות אם שם המארח זהה לשם המארח המקומי. אם שני השמות שונים, מנותח הקובץ HOSTS. אם שם המארח נמצא בקובץ HOSTS הוא מתורגם לכתובת IP.

   אם לא ניתן את שם המארח, ולא מוגדרת אף שיטת הסדרה אחרת - כגון DNS, שרת שמות NetBIOS או קובץ LMHOSTS - התהליך נעצר והמשתמש מקבל הודעת שגיאה.
3. לאחר שכתובת המארח מתורגמת לכתובת IP, נעשה ניסיון להסדיר את כתובת ה-IP של מארח היעד לכתובת החומרה שלו.

   אם מארח היעד נמצא ברשת המקומית, מאחזר ARP את כתובת החומרה שלו ממטמון ARP, או על ידי שידור רחב של כתובת ה-IP של מארח היעד.

אם מארח היעד נמצא ברשת מרוחקת, מאחזר ARP את כתובת החומרה של נתב (Router) והבקשה מנותבת למארח היעד.



תרשים 6.1 הסדרת כתובת IP של מארח היעד לכתובת החומרה שלו

הסדרת שמות באמצעות שרת DNS

שרת DNS הוא מסד נתונים מקוון מרכזי המשמש ברשתות IP להסדרת שמות מארחים לכתובות IP. ‏Windows 2000 יכולה לשתמש כלקוח DNS ומשפחת השרתים של Windows 2000 מספקת את שירותי השרת של DNS. הסדרת שמות באמצעות שרת DNS דומה מאוד לאופן בו מתבצע הדבר באמצעות קובץ HOSTS.

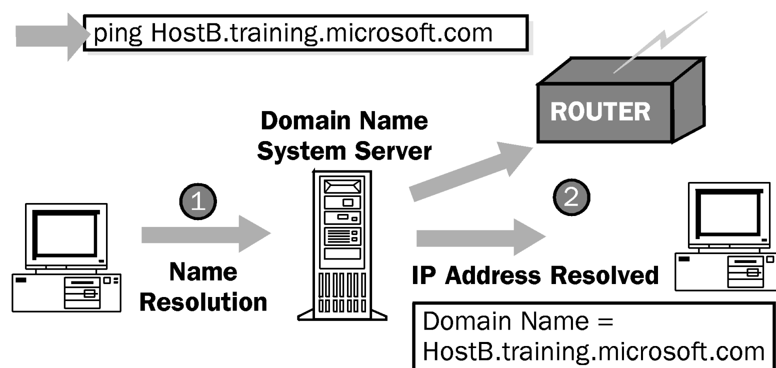
אם Windows 2000 מוגדרת להסדרת שמות באמצעות שרת DNS, היא נעזרת בשני צעדים להסדרת שם מארח, כפי שמוצג בהליך הבא ומתואר בתרשים 6.2, בהתאמה:

1. כאשר משתמש מקליד פקודה תוך שימוש ב-FQDN או שם מארח (Host Name), מתבצע תהליך הסדרה באמצעות הקובץ HOSTS כצעד ראשון. אם כתובת ה-IP אינה יכולה להיות מוסדרת באמצעות הקובץ HOSTS, נשלחת בקשה לשרת ה-DNS, כדי שיאתר את השם במסד הנתונים שלו ויתרגם אותו לכתובת IP.

   אם שרת ה-DNS אינו מגיב לבקשה, מתבצעים ניסיונות חוזרים (בהפרשי זמן של 1, 2, 2 ו-4 שניות בין אחד לשני). אם שרת ה-DNS אינו מגיב לחמישה ניסיונות אלה ולא הוגדרו שיטות הסדרה נוספות, כגון שרת שמות NetBIOS או קובץ LMHOSTS, התהליך נעצר ומתקבלת הודעת שגיאה.

2. לאחר שהוסדר שם המארח, מאחזר ARP את כתובת החומרה. אם מארח היעד נמצא ברשת המקומית, מאחזר ARP את כתובת החומרה שלו על ידי התייעצות עם מטמון ARP, או על ידי Broadcast של כתובת ה-IP. אם מארח היעד נמצא ברשת מרוחקת, מאחזר ARP את כתובת החומרה של נתב שיכול להעביר את הבקשה.

   אם שרת ה-DNS נמצא ברשת מרוחקת, חייב ARP לאחזר את כתובת החומרה של הנתב, לפני שהסדרת השמות תוכל להתבצע.



תרשים 6.2 הסדרת שם מארח באמצעות שרת DNS

שיטות Microsoft להסדרת שמות מארחים

ניתן להגדיר את Windows 2000 להסדרת שמות תוך שימוש בשרת שמות NetBIOS, Broadcast והקובץ LMHOSTS, וזאת בנוסף להסדרה באמצעות הקובץ HOSTS ושרת DNS. אם נכשלה אחת משיטות אלו, מספקת השיטה האחרת גיבוי, כפי שניתן לראות בדוגמה הבאה, ובתרשים 6.3 שלאחריה. אם הוגדרו WINS והקובץ LMHOSTS, יהיה סדר ההסדרה כדלקמן:

1. כאשר משתמש מקליד פקודה המתייחסת לשם מארח, בודקת Windows 2000 אם שם המארח זהה לשם המארח המקומי. אם כך הוא הדבר, השם מוסדר והפקודה מבוצעת מבלי לחולל פעילות רשת כלשהי.

2. אם שם המארח אינו זהה לשם המארח המקומי, מנותח הקובץ HOSTS. אם שם המארח נמצא בקובץ HOSTS הוא מתורגם לכתובת IP ומתבצעת הסדרת כתובות.

3. אם שם המארח אינו ניתן להסדרה באמצעות הקובץ HOSTS, שולח מארח המקור בקשה לשרתי שמות ה-Domains המוגדרים בו. אם שם המארח אותר על ידי שרת DNS, הוא מוסדר לכתובת IP ומתבצעת הסדרת כתובות.

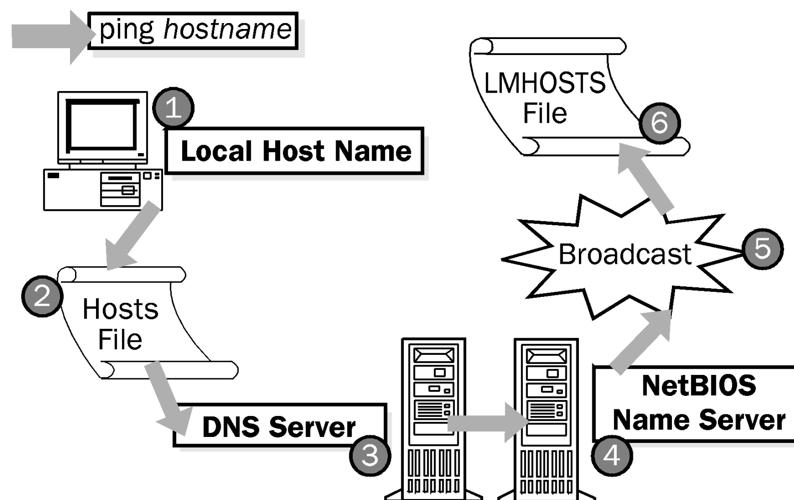
   אם שרת ה-DNS אינו מגיב לבקשה, מתבצעים ניסיונות חוזרים (בהפרשי זמן של 1, 2, 2 ו-4 שניות בין אחד לשני).

4. אם שרת ה-DNS אינו מצליח להסדיר את שם המארח, בודק מארח המקור את מטמון שמות NetBIOS המקומי, וזאת לפני שינסה לבצע שלושה ניסיונות להתקשרות עם שרתי שמות NetBIOS המוגדרים בו. אם שם המארח נמצא במטמון שמות NetBIOS או על ידי שרת שמות NetBIOS, הוא מוסדר לכתובת IP ומתבצעת הסדרת כתובות.

5. אם שם המארח אינו מוסדר על ידי שרת שמות NetBIOS, מחולל מארח המקור שלוש הודעות שידור רחב (Broadcast) לרשת המקומית. אם שם המארח נמצא ברשת המקומית הוא מוסדר לכתובת IP ומתבצעת הסדרת כתובות.

6. אם שם המארח אינו מוסדר תוך שימוש בשידור רחב, מנותח הקובץ LMHOSTS המקומי. אם שם המארח נמצא בקובץ LMHOSTS הוא מוסדר לכתובת IP ומתבצעת הסדרת כתובות.

אם אף אחת מהשיטות אינה מסדירה את שם המארח, ציון כתובת ה-IP תהיה הדרך היחידה לתקשר עם המארח האחר.



תרשים 6.3 שיטות גיבוי להסדרת שמות מארחים

סיכום שיעור

שם מארח משמש לזיהוי מארח TCP/IP או Default Gateway. הסדרת שם מארח (Host Name Resolution) הוא תהליך של מיפוי שם מארח לכתובת IP. הדבר נחוץ כדי ש-ARP יוכל להסדיר כתובות IP לכתובות החומרה.

שיעור 3: הקובץ HOSTS

כעת, משלמדת אודות האופן בו מוסדרים שמות מארחים תוך שימוש בשיטות השונות, יוצג בפניך הקובץ HOSTS. בשיעור זה תשנה את הקובץ HOSTS כך ששמות המארחים יוסדרו כיאות.

לאחר שיעור זה, תוכל

- להגדיר ולהשתמש בקובץ HOSTS.

זמן לימוד משוער: 15 דקות

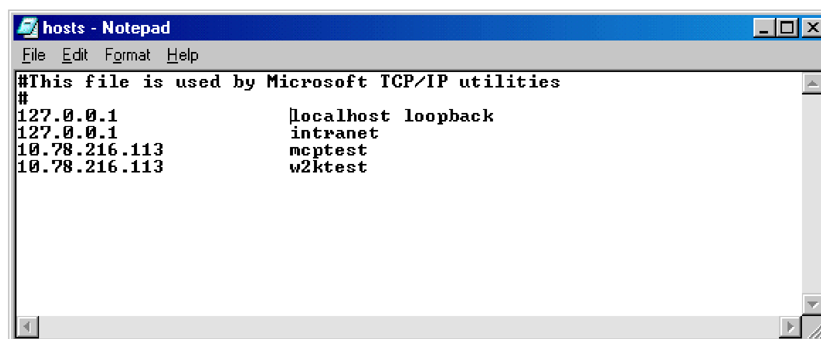
הקובץ HOSTS

הקובץ HOSTS הוא קובץ סטטי המשמש למיפוי שמות מארחים לכתובות IP. קובץ זה תואם לקובץ HOSTS של UNIX. הקובץ HOSTS משמש את הפקודה PING ויישומי TCP/IP אחרים, כדי להסדיר שם מארח לכתובת IP שלו. הקובץ HOSTS יכול לשמש להסדרת שמות NetBIOS (Microsoft TCP/IP-32-Specific).

קובץ HOSTS חייב להיות קיים בכל מחשב. רשומה אחת מורכבת מכתובת IP המקבילה לשם מארח אחד או יותר. כברירת מחדל קיימת בקובץ רשומה עבור שם המארח localhost. הקובץ HOSTS מנותח בכל פעם שמתבצעת התייחסות לשם מארח. שמות נקראים בשיטה הלינארית. השמות בהם נעשה השימוש התכוף ביותר צריכים להיות קרובים יותר לתחילת הקובץ.

הערה ניתן לערוך את הקובץ HOSTS בכל עורך טקסט רגיל. הוא ממוקם בתיקיה \SystemRoot\System32\Drivers\Etc. כל רשומת מארח מוגבלת ל-255 תווים, והרשומות אינן תלויות-רישיות.

תרשים 6.4 מציג דוגמה של תוכן קובץ HOSTS.



תרשים 6.4 קובץ HOSTS

- מאפשר לשייך מספר שמות מארחים לאותה כתובת IP. שים לב שניתן להתייחס לשרת בכתובת IP 172.16.94.97 בשם ה-Domain המלא שלו (FQDN, rhino.microsoft.com) או בכינוי שלו (rhino). דבר זה מאפשר למשתמש במחשב זה להתייחס לשרת זה תוך שימוש בכינוי rhino, במקום להקליד את כל ה-FQDN.
- רשומות עשויות להיות תלויות-רישיות, בהתאם לפלטפורמה. רשומות בקובץ HOSTS בחלק ממערכות ההפעלה של UNIX הן תלויות-רישיות. רשומות בקובץ HOSTS במערכות מבוססות-Windows 2000 או מערכות Windows 2000 אינן תלויות-רישיות.

יתרון השימוש בקובץ HOSTS

היתרון שבשימוש בקובץ HOSTS טמון בכך שהוא ניתן להתאמה אישית עבור משתמש. כל משתמש יכול ליצור איזה רשומות שהוא רוצה, כולל כינויים שיקלו עליו לזכור לצורך גישה תכופה למשאבים. אבל, הניהול הפרטני של הקובץ HOSTS אינו מהווה פתרון מתאים לשמירה על מספר גדול של מיפויי FQDNs.

תרגול: עבודה עם קובץ HOSTS ו-DNS

בתרגול זה תגדיר ותשתמש בקובץ HOSTS, תגדיר את Windows 2000 לשימוש עם שרת DNS ותזהה בעיות הקשורות להסדרת שמות מארחים ושמות DOMAINS. בחלקו הראשון של הליך זה, תוסיף מיפוי שם מארח/כתובת IP לקובץ HOSTS שלך, ואז תיעזר בקובץ לצורך הסדרת השמות.

בהליך זה, אתה קובע את המארח המקומי המשמש ליישומי TCP/IP כגון PING.

➢ כדי לקבוע את שם המארח המקומי

1. פתח חלון שורת הפקודה (Command Prompt).
2. במנחה שורת הפקודה הקלד hostname, והקש Enter.

   בחלון מוצג שם המארח המקומי.

בהליך הבא תבצע PING לשם המארח המקומי, כדי לוודא שהמערכת שלך יכולה להסדיר שמות מארחים מקומיים ללא רשומות נוספות בקובץ HOSTS.

➢ כדי לבצע PING לשם המארח המקומי

1. הקלד ping Server1 (כאשר Server1 הוא שם המחשב שלך), והקש Enter.

   מה היתה התגובה?

בצע את ההליך הבא במחשב Server1, כדי לנסות לבצע PING לשם מחשב מקומי.

➢ כדי לבצע PING לשם מחשב מקומי

1. הקלד את הפקודה ping computertwo, והקש Enter.

מה היתה התגובה?

➢ כדי להוסיף רשומה לקובץ HOSTS במחשב Server1

1. עבור לתיקיה Etc על ידי הקלדת הפקודה הבאה:

```
cd %systemroot%\system32\drivers\etc
```

2. היעזר בעורך טקסט רגיל כדי לשנות את הקובץ HOSTS. עשה זאת על ידי הפקודה:
notepad hosts

3. הוסף לקובץ HOSTS רשומה עבור המחשב computertwo. רשומה זו תכלול כתובת IP, לאחריה רווח ולאחריו שם המארח.

4. שמור את הקובץ וצא מעורך הטקסט.

➢ כדי להשתמש בקובץ HOSTS לשם הסדרת שמות

1. הקלד ping computertwo, והקש Enter.

מה היתה התגובה?

סיכום שיעור

הקובץ HOSTS הוא קובץ טקסט אותו ניתן לערוך באמצעות כל עורך טקסט רגיל (כגון Notepad). הקובץ HOSTS ממפה שמות מארחים לכתובות IP והוא תואם לקובץ HOSTS של UNIX. אם הרשת שלך משתמשת בקובץ HOSTS לשם הסדרת שמות מארחים ואינך מצליח להתחבר למחשב אחר באמצעות שם המארח שלו, ייתכן שהקובץ HOSTS שלך מכיל רשומה לא תקינה. חפש בקובץ HOSTS שלך אחר שם המארח של המחשב האחר, ודא כי קיימת רשומה אחת בלבד לכל שם מארח ואז ודא כי הרשומה עבור שם המארח של המחשב האחר אכן תקינה. למידע נוסף אודות הקובץ HOSTS ראה דוגמה שלו בתיקיה %SystemRoot%\System32\Drivers\Etc.



שאלות סיכום

השאלות הבאות נועדו לחזק את הנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות על שאלה, עיין בשיעור המתאים ונסה את השאלה שנית. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואחר כך בעברית.

Answering the following questions will reinforce key information presented in this chapter. If you are unable to answer a question, review the appropriate lesson and then try the question again. Answers to the questions can be found in Appendix A, "Questions and Answers."

1. What is a host name?
2. What is the purpose of a host name?
3. What does a HOSTS file entry consist of?
4. During the name resolution process, what occurs first: ARP resolution or host name resolution?

1. מהו שם מארח?
2. מהי מטרתו של שם המארח?
3. ממה מורכבת רשומת הקובץ HOSTS?
4. בעת תהליך הסדרת השמות, מה מתרחש ראשון: הסדרת ARP או הסדרת שם מארח?

פרק 7

יישום DNS (Domain Name System)

אודות פרק זה

בפרק זה תלמד כיצד משמש DNS (**D**omain **N**ame **S**ystem) להסדרת שמות ברשת המקומית (LAN) וברשת האינטרנט הציבורית. Windows 2000 כוללת גירסה משופרת של DNS. למידע נוסף אודות האופן בו משתמשת Windows 2000 ב-DNS, קרא את הפרק הבא. פרק זה נועד לספק לך סקירה לגבי DNS ואופן יישום שירות זה בסביבת Windows 2000. לקראת סופו של הפרק תהיה מסוגל לזהות את רכיביו העיקריים של DNS, להתקין ולהגדיר אותו, ולאתר ולטפל בתקלות בשירות DNS של Windows 2000.

לפני שתתחיל

להשלמת פרק זה צריך שיהיה ברשותך:

- מחשב בו מותקנת מערכת ההפעלה Windows 2000 Server, ובה מוגדר פרוטוקול TCP/IP.

שיעור 1 : סקירת DNS

DNS דומה לספר טלפונים. לכל מחשב באינטרנט יש גם שם מארח וגם כתובת IP (**I**nternet **P**rotocol). בדרך כלל, כשאתה מעוניין להתחבר למחשב אחר עליך להקליד שם מארח. אז, יוצר המחשב שלך קשר עם שרת DNS אשר מצידו מבצע השוואה של שם המארח שסיפקת לכתובת IP ממשית. אותה כתובת IP משמשת משלב זה לצורך ההתקשרות עם המחשב המרוחק. שיעור זה מתאר את הארכיטקטורה ואת מבנה ה-DNS.

לאחר שיעור זה, תוכל

- לתאר את מבנה, ארכיטקטורה ומרכיבי ה-DNS.
- להסביר מדוע DNS משמש להסדרת שמות וכתובות IP.

זמן לימוד משוער: 25 דקות

מקורות ה-DNS

לפני שהחל יישומו של DNS היה השימוש בשמות ידידותיים של מחשבים מתבצע באמצעות קבצי HOSTS שהכילו רשימה של שמות וכתובות IP משויכות. באינטרנט, נוהל קובץ זה במרוכז, וכל נקודה מרכזית ברשת היתה מורידה מדי פעם עותק מעודכן. ככל שגדל מספרם של המחשבים באינטרנט, הפך פתרון זה לבלתי יעיל. כתוצאה מכך, עוצב DNS כדי להחליף את קובץ HOSTS המנוהל באופן פרטני במסד נתונים מבוזר שיאפשר מרחב שמות היררכי, ביזור הניהול, סוגי נתונים ברי-הרחבה, בסיס נתונים בגודל כמעט אין-סופי וביצועים משופרים. DNS הוא שירות השם עבור כתובות אינטרנט המתרגם שמות ידידותיים של Domains לכתובות IP מספריות. למשל, הכתובת www.microsoft.com תתורגם לכתובת 207.46.230.218. DNS דומה במשהו לספר הטלפונים. המשתמש מחפש את שם האדם או החברה איתו הוא מעוניין ליצור קשר ומשייך לשם זה מספר טלפון. בדומה, מחשב מארח מבצע שאילתה לפי שם המחשב וה- Domain Name Server משייך לשם זה כתובת IP.

יישומה של Microsoft לשרת DNS הפך לחלק בלתי נפרד ממערכת ההפעלה Windows NT Server 4.0, ומסורת זו ממשיכה גם ב- Windows 2000.

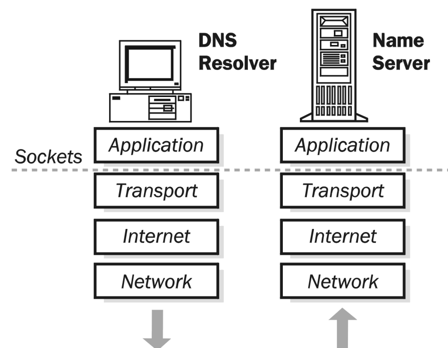
DNS ו- Windows 2000

בנוסף לתיפקוד המסורתי כמסדיר שמות אינטרנט, DNS הוא שירות השמות העיקרי של Windows 2000. ביסודו זהו מסד נתונים אמין ביותר, הירכי, מבוזר וברי-הרחבה. לקוחות Windows 2000 משתמשים ב-DNS להסדרת שמות ואיתור שירותים, כולל איתור Domain Controllers לצורך הכניסה למערכת (Log On). DNS ב-Windows 2000 מספק יישום ייחודי של שרת DNS אשר מסוגל לפעולה משולבת מלאה עם שרתי DNS אחרים. למידע נוסף אודות הגירסה של DNS המצורפת ל- Windows 2000 קרא פרק הבא.

כיצד פועל DNS

מטרתו של מסד הנתונים של DNS היא לתרגם שמות מחשבים לכתובות IP, כפי שמתואר בתרשים 7.1. ב-DNS נקראים הלקוחות Resolvers (מיישבים) והשרתים נקראים שרתי שמות (Name Server). DNS פועל באמצעות שלושה רכיבים עיקריים: Resolvers, שרתי שמות (Name Servers) ו- Domain Name Space. בתקשורת DNS בסיסית, שולח Resolver שאילתה לשרת שמות. שרת השמות מחזיר את המידע המבוקש, מצביע (Pointer) לשרת שמות אחר, או שהוא מחזיר הודעת כשל במידה ואין אפשרות למלא אחר הבקשה.

DNS ממפה לשכבת היישום (Application Layer) ומשתמש ב-UDP (**U**ser **D**atagram **P**rotocol) וב-TCP (**T**ransmission **Co**ntrol **P**rotocol) כפרוטוקולים הבסיסיים לביצוע. מטעמי ביצועים, שולחים ה-Resolvers שאילתות UDP לשרתים תחילה, ואז פונים ל-TCP אם מתרחש קיצוץ (Trunction) של הנתונים המוחזרים.



תרשים 7.1 מיישבים ושרתי שמות

Resolvers

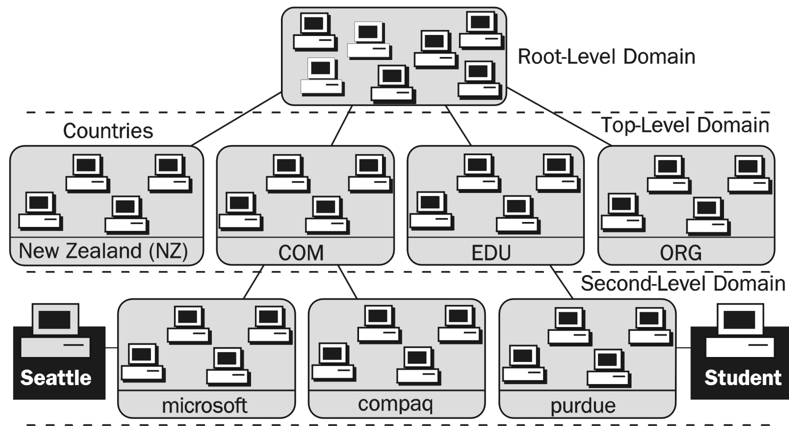
Resolver (מיישב) מספק ללקוחות מידע אודות כתובות של מחשבים אחרים ברשת. פעולתו של ה-Resolver היא להעביר בקשות לשמות בין היישומים לבין שרתי השמות. בקשת השם מכילה שאילתה, כגון כתובת ה-IP של אתר אינטרנט. במקרים רבים בנוי ה-Resolver כחלק מהיישום, או שהוא מופעל במחשב המארח כשגרת ספריה (Library Routine). ה-Resolvers שולחים תחילה שאילתות UDP לשרתים, כדי לשפר את הביצועים, ופונים ל-TCP רק במידה והנתונים המוחזרים מקוצצים.

שרתי שמות

שרת שמות (Name Server) מכיל נתוני כתובות לגבי מחשבים אחרים ברשת. מידע זה יכול להינתן למחשב לקוח המבצע בקשה משרת השמות. אם שרת השמות אינו מסוגל להסדיר את הבקשה הוא יכול להעביר את הבקשה לשרת שמות אחר. שרתי השמות מקובצים לרמות שונות, הנקראות Domains. Domain הוא קבוצה לוגית של מחשבים ברשת גדולה. גישה לכל מחשב בקבוצה נתונה נשלטת בידי אותו שרת.

מבנה DNS

DNS (**D**omain **N**ame **S**pace) הוא קיבוץ הירככי של שמות, כפי שניתן ללמוד מתרשים 7.2.



תרשים 7.2 מרחב שמות ב- Domain מחולק לרמות

Root Domain

Domains מגדירים רמות שונות של סמכות במבנה הירככי. חלקה העליון (ראש) של ההירככיה נקרא Root Domain. התייחסות ל-Root Domain מבוטאת על ידי נקודה (**.**).

Top-Level Domains

ה-domains הבאים נחשבים, נכון לימים אלה, כ- Top-Level Domains :

- **com** חברה/ארגון מסחרי
- **edu** מוסד חינוכי ואוניברסיטאות
- **org** מוסד ללא כוונת רווח (מלכ"ר)
- **net** רשתות (המהוות את תשתית היסוד, Backbone, של האינטרנט)
- **gov** ארגונים ממשלתיים לא צבאיים
- **mil** ארגונים צבאיים ממשלתיים
- **num** מספרי טלפון
- **arpa** היפוך DNS (Reverse DNS)
- **xx** קוד מדינה בן שתי אותיות (כגון il, tw או ae)

Domains ברמה העילית יכולים להכיל Domains ברמה משנית ומארחים.

הערה ועדת קהילת האינטרנט (Internet Society Committee) מתכננת ליצור מספר Domains נוספים ברמה העילית, כגון firm ו-web.

Second-Level Domains

תחומים ברמה המשנית (Second-Level Domains) יכולים להכיל מארחים וגם Domains אחרים, הנקראים Subdomain. לדוגמה, ה-Domain של Microsoft, microsoft.com, יכול להכיל מחשבים, כגון ftp.microsoft.com ו- Subdomains כגון dev.microsoft.com. ה- Subdomain של dev.microsoft.com יכול להכיל מארחים, כגון ntserver.dev.microsoft.com.

שמות מארחים

שם ה- Domain משמש בצירוף לשם המארח כדי ליצור FQDN (**F**ully **Q**ualified **D**omain **N**ame) עבור מחשב זה. ה-FQDN הוא שם המארח, אחריו נקודה (.) ואחריה שם ה- Domain. יכול להיות fileserver1.microsoft.com, כאשר fileserver1 הוא שם המארח ואילו microsoft.com הוא שם ה- Domain.

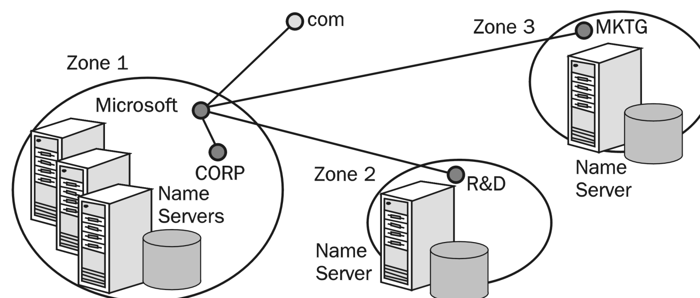
Zones

יחידת הניהול של DNS נקראת אזור (Zone). אזור הוא עץ משנה (Subtree) של מסד הנתונים של DNS אשר מנוהל כיישות יחידה ונפרדת אחת. הוא יכול להכיל Domain יחיד או Domain עם Subdomain. את ה- Subdomains ברמות הנמוכות יותר של האזור ניתן לחלק ל- Zones נפרדים נוספים.

Zones of Authority

אזור סמכות (Zone of Authority) הוא החלק ב-DNS (**D**omain **N**ame **S**pace) בעבורו אחראי שרת שמות מסוים. שרת השמות מאחסן את כל מיפויי הכתובות של ה-DNS באזור, ונותן מענה לשאילתות של לקוחות המכוונים לשמות אלה. אזור הסמכות של שרת השמות מקיף לפחות Domain אחד. ל- Domain זה מתייחסים כאל Zone's Root Domain. יכול להיות לך גם שרת DNS משני, אשר מסוגל להעתיק נתוני Domain דרך הרשת משרת DNS עיקרי לו יש סמכות על לפחות אזור אחד. פעולה זו נקראת העברת אזור (Zone Transfer).

כפי שניתן לראות בתרשים 7.3, microsoft.com הוא Domain, אבל ה- Domain כולו אינו נשלט בידי קובץ אזור (Zone File) אחד. חלק מה- Domain ממוקם בקובץ אזור נפרד עבור DEV.MICROSOFT.COM. פיצול Domains בין מספר Zones יכול להיות הכרחי לשם ביזור ניהול ה-Domain לקבוצות שונות, או לצורך מיטוב יעילות שכפול נתונים (Data Replication).



תרשים 7.3 Domains המתפרסים על מספר Zones

תפקידי שרת השמות

ניתן להגדיר את שרתי השמות של DNS כך שיבצעו תפקידים שונים, דבר שישפיע על האופן בו הם מאחסנים ומתחזקים את מסד נתוני השמות שלהם. שרת DNS יכול להיות עיקרי (Primary) או שרת DNS משני (Secondary) לשרת DNS אחר, או שהוא שרת DNS הפועל בסביבת מערכת הפעלה שונה, כגון UNIX. המספר המינימלי המומלץ של שרתי DNS שצריך כדי לשרת כל אזור הוא שניים - עיקרי ומשני. גם השרת העיקרי וגם השרת המשני צריכים לספק Redundancy של מסד הנתונים, ומידה מסוימת של Fault Tolerance.

שרתי שמות עיקריים

שרת שמות עיקרי (Primary Name Server) הוא שרת DNS המקבל את הנתונים עבור ה-Zones שלו מקבצי מסד הנתונים המקומיים של ה-DNS. כאשר מתבצע שינוי לנתוני האזור, כגון האצלת (Delegation) חלק מהאזור לסמכותו של שרת DNS אחר, או הוספת מארחים באזור, חייב השינוי להתבצע בשרת DNS העיקרי, כדי שהמידע החדש יתווסף לקובץ האזור המקומי.

שרתי שמות משניים

שרת שמות משני (Secondary Name Server) מקבל את קובץ נתוני האזור שלו משרת ה-DNS העיקרי לו יש סמכות על אזור זה. שרת ה-DNS העיקרי שולח עותק של קובץ האזור לשרת ה-DNS המשני. תהליך זה נקרא העברת אזור (Zone Transfer).

קיימות שלוש סיבות להחזקת שרתי שמות משניים:

- **Redundancy.** לכל אזור חייבים להיות לך לפחות שרת עיקרי אחד ושרת משני אחד. מחשבים אלה צריכים לעמוד בפני עצמם עד כמה שניתן. בדרך כלל, עליך לנסות ולהגדיר את שרתי השמות העיקרי והמשני בשתי Subnets שונות, כדי להמשיך ולספק תמיכה לשאילתות שמות DNS במידה ו- Subnet אחת קורסת.
- **גישה מהירה יותר למיקומים מרוחקים.** אם יש לך מספר לקוחות במיקומים מרוחקים, עובדת קיומו של שרת שמות משני (או שרתי שמות אחרים ב-Subdomains) מונעת מלקוחות אלה מלתקשר דרך קישורים איטיים לצורך הסדרת שמות. הם פשוט פונים לשרת הקרוב אליהם.
- **הפחתת עומס.** שרתי שמות משניים מפחיתים את העומס משרת השמות העיקרי.

מכיון שהמידע על כל אזור מאוחסן בקבצים נפרדים, מוגדרת העיקריות או המשניות ברמת האזור. הדבר אומר ששרת שמות מסוים יכול להיות שרת שמות עיקרי ל- Zones מסוימים, בעודו משמש כשרת שמות משני ל- Zones אחרים.

שרתי שמות ראשיים

כאשר אתה מגדיר בשרת שמות אזור כאזור משני (Secondary Zone), עליך לייעד שרת שמות אחר, ממנו יש לאחזר את מידע האזור. המקור למידע האזור עבור שרת שמות משני בהירככיית ה-DNS נקרא שרת שמות ראשי (Master Name Server). שרת שמות ראשי יכול להיות שרת שמות עיקרי או משני עבור האזור המבוקש. כאשר מאותחל שרת שמות משני הוא יוצר קשר עם שרת השמות הראשי שלו ומתחיל בביצוע העברת אזור (Zone Transfer) עם שרת זה.

שרתי מטמון-בלבד

למרות שכל שרתי שמות DNS מטמינים (Cache) שאילתות אותן הם מסדירים, שרתי מיטמון-בלבד (Caching-Only Servers) הם שרתי שמות DNS שרק מבצעים שאילתות, מטמינים את התשובות ומחזירים את התוצאות. במילים אחרות, הם אינם בעלי סמכות באיזה מבין ה-Domains (שום מידע אזור אינו נשמר באופן מקומי) והם מכילים רק מידע שהם עצמם הטמינו בעת הסדרת שאילתות.

כאשר תשקול את השימוש בשרת כגון זה, קח בחשבון שכאשר שרת כזה מאותחל לראשונה, לא מוטמן בו מידע כלשהו ועליו לאגור את המידע במשך הזמן, כפי שמתבקש משירותיו. פחות תעבורה מתחוללת בין השרתים, מפני שהשרת אינו מבצע העברות אזור. הדבר חשוב אם יש לך קישורים איטיים בין אתרים.

סיכום שיעור

DNS נוצר כשיפור לשיטה הישנה להסדרת שמות מארחים לכתובות IP באינטרנט. ב-DNS, לקוח (הנקרא Resolver) שולח שאילתה לשרת שמות. שרתי השמות (Name Servers) מקבלים בקשות לשמות, ומסדירים (מתרגמים) את שמות המחשבים לכתובות IP. ה-DNS (Domain Name Space) הוא קיבוץ היררכי של Root-Level Domains, Top-Level Domains, Secondary-Level Domains ושמות מארחים (Host Names). שרתים מסוימים, האחראים לחלקים של DNS, נקראים אזורי סמכות (Zones of Authority).

שיעור 2: הסדרת שמות וקבצי DNS

קיימים שלושה סוגי שאילתות אותן יכול ה- Resolver לבצע לשרת DNS: רקורסיבית (Recursive), איטרטיבית (Iterative) ואינברסית (Inverse). שרתים אלה מאחסנים את מידע DNS בארבעה קבצים אפשריים: מסד נתונים (Database), חיפוש לאחור (Reverse Lookup), מטמון (Cache) או אתחול (Boot).

לאחר שיעור זה, תוכל

- להסביר כיצד פועלות שאילתות רקורסיביות, איטרטיביות ואינברסיות.
- להסביר כיצד מוטמנות שאילתות אלו לשימושן של שאילתות עתידיות.

זמן לימוד משוער: 10 דקות

שאילתות רקורסיביות

בשאילתה רקורסיבית, נדרש שרת השמות בו מבוצעת השאילתה להגיב עם המידע המבוקש, או בהודעת שגיאה המצהירה כי מידע מהסוג המבוקש לא קיים או ששם ה-Domain שצוין אינו קיים. שרת השמות אינו יכול להעביר בקשה לשרת שמות אחר.

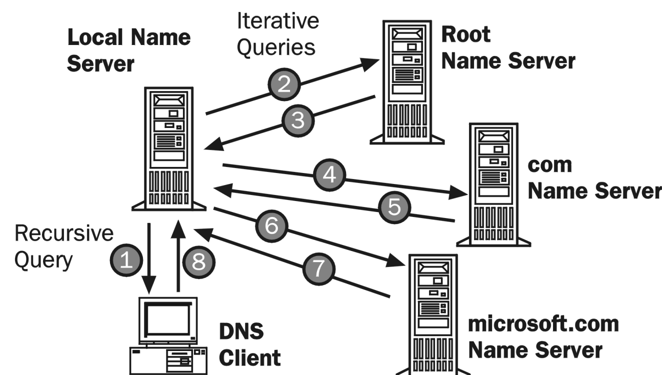
שאילתות איטרטיביות

במקרה של שאילתה איטרטיבית, מחזיר שרת השמות בו מבוצעת השאילתה את התשובה הטובה ביותר הידועה לו באותו רגע נתון. תשובה זו יכולה להיות שמו המוסדר של המחשב, או הפנייה לשרת שמות אחר שייתכן שיוכל לענות על שאילתת הלקוח המקורית.

תרשים 7.4 מציג דוגמה לשאילתה רקורסיבית ולשאילתה איטרטיבית. בדוגמה זו, לקוח בארגון מבצע שאילתה לשרת ה-DNS שלו, לגבי כתובת ה-IP של www.microsoft.com.

1. ה- Resolver שולח שאילתת DNS רקורסיבית לשרת ה-DNS המקומי שלו ומבקש את כתובת ה-IP של www.microsoft.com. שרת השמות המקומי הוא זה האחראי על הסדרת השם, ואינו יכול להפנות את ה- Resolver לשרת שמות אחר.
2. שרת השמות המקומי בוחן את ה- Zones שלו ואינו מאתר אזור התואם לשם ה-Domain המבוקש. אז, הוא שולח לשרת שמות ברמת השורש שאילתה איטרטיבית עבור www.microsoft.com.
3. לשרת השמות ברמת השורש יש סמכות על Root Domain והוא ישיב את כתובת ה-IP של שרת שמות עבור ה- Domain ברמה העילית com.
4. שרת השמות המקומי שולח שאילתה איטרטיבית עבור www.microsoft.com לשרת השמות של com.
5. שרת השמות של com מגיב עם כתובת ה-IP של שרת השמות המשרת את ה- Domain microsoft.com.

6. שרת השמות המקומי שולח שאילתה איטרטיבית עבור www.microsoft.com לשרת השמות של microsoft.com.
7. שרת השמות של microsoft.com מגיב עם כתובת ה-IP המשויכת ל-www.microsoft.com.
8. שרת השמות המקומי שולח את כתובת ה-IP של www.microsoft.com חזרה ל-Resolver המקורי.



תרשים 7.4 שאילתה רקורסיבית ושאילתה איטרטיבית

שאילתות אינברסיות

בשאילתה אינברסית (הפוכה) שולח ה- Resolver לשרת השמות בקשה להסדיר את שם המארח עם כתובת IP ידועה. לא קיימת התאמה בין שמות המארח לבין כתובת ה-IP שבמרחב השמות של ה-DNS. בשל כך, רק חיפוש יסודי בכל ה-Domains יבטיח את התשובה הנכונה.

כדי למנוע חיפוש מייגע בכל ה- Domains במקרה של שאילתה אינברסית, נוצר Domain מיוחד בשם in-addr.arpa. הרכיבים ב-in-addr.arpa Domain נקראים על פי המספרים שבייצוג הדצימלי המנוקד (Dotted Decimal) של כתובות IP. מאחר וכתובות IP הופכות להיות נקודתיות יותר כאשר הן נקראות משמאל לימין, ואילו שמות Domains הופכים להיות פחות נקודתיים כאשר הם נקראים משמאל לימין, יש להפוך את סדר האוקטטים (Octet) של כתובת IP כאשר בונים את ה-in-addr.arpa Domain. בסידור כגון זה, ניתן להאציל את סמכות הניהול של האיברים הנמוכים יותר ב-in-addr.arpa Domain לארגונים, כפי שמוקצות להן מחלקות כתובות ה-IP - A, B או C.

לאחר שנבנה ה-in-addr.arpa Domain, רשומות משאבים מיוחדות, הנקראות מצביעים (Pointer ,PTR), נוספות ומשויכות לכתובת ה-IP ולשם המארח התואם. למשל, כדי למצוא את שם המארח התואם לכתובת 157.55.200.51, מבצע ה- Resolver שאילתה לשרת ה-DNS אחר רשומת PTR עבור 51.200.55.157.in-addr.arpa. רשומת PTR שתימצא מכילה את שם המארח התואם לכתובת 157.55.200.51. מידע זה נשלח חזרה ל- Resolver. חלק מניהול שרת שמות DNS כולל להבטיח שתיווצר רשומת PTR עבור המארחים.

Time-To-Live ו- Caching

כאשר שרת שמות מעבד שאילתה רקורסיבית, ייתכן שיימצא הצורך לשלוח מספר שאילתות כדי למצוא את התשובה. שרת השמות מטמין (Cache) את כל המידע שהוא מקבל בעת תהליך זה למשך זמן המוגדר בנתונים המוחזרים. למשך הזמן קוראים **T**ime-**T**o-**L**ive, TTL. מנהל שרת השמות של האזור המכיל את המידע קובע את משך ה-TTL עבור הנתונים. ערכי TTL קטנים יותר יבטיחו שנתונים אודות ה- Domain יהיו עקביים יותר, אם מידע זה משתנה לעיתים קרובות. אבל, דבר זה גם מגדיל את העומס על שרתי השמות.

לאחר שהנתונים מוטמנים על ידי שרת ה-DNS, עליו להתחיל להקטין את ערך ה-TTL, כדי שהוא ידע מתי עליו למחוק מידע זה מהמטמון. אם נכנסת שאילתה אותה ניתן למלא באמצעות מידע זה, ערך ה-TTL המוחזר יחד עם המידע הוא משך הזמן הנוכחי, לפני שמידע זה יימחק מהמטמון של שרת ה-DNS. גם ל- Resolvers יש מטמון והם מכבדים את ערכו של TTL, כך שהם יודעים מתי פג תוקפו של המידע.

קבצי תצורת DNS

DNS הוא מסד נתונים מבוזר היררכי. מסד הנתונים עצמו מורכב מרשומות משאבים, אשר בעיקרן מורכבות משם DNS, סוג רשומה וערכי נתונים המשויכים עם סוג הרשומה. למשל, הרשומות השכיחות ביותר במסד הנתונים של DNS הן רשומות כתובות, בהן שם של רשומת כתובת הוא שם של מחשב, והנתונים ברשומה הם כתובת ה-TCP/IP של אותו מחשב.

כדי להסדיר שמות, מתייעצים השרתים עם ה- Zones שלהם (הנקראים גם קבצי מסד נתוני DNS, DNS Databse Files, או בקיצור קבצי db, db Files). ה- Zones מכילים רשומות משאבים (RR, **R**esource **R**ecords) המכילות מצידן את המידע אודות המשאבים המשויכים ל- DNS domain. לדוגמה, RRs מסוימות ממפות שמות ידידותיים לכתובות IP, ואחרות ממפות כתובות IP לשמות ידידותיים.

רשומת Start Of Authority

הרשומה הראשונה בכל מסד נתונים חייבת להיות רשומת **S**tart **O**f **A**uthority (SOA). SOA מגדירה את הפרמטרים הכלליים עבור אזור DNS.
השורות הבאות הן דוגמה לרשומת SOA:

```
@       IN      SOA     nameserver.example.microsoft.com
postmaster.example.microsoft.com.  (
                        1           ;   serial number
                        3600        ;   refresh  [1h]
                        600         ;   retry    [10m]
                        86400       ;   expire   [1d]
                        3600 )      ;   min TTL  [1h]
```

הכללים הבאים נכונים לגבי כל רשומות SOA:

- הסימן @ בקובץ מסד נתונים מציין "שרת זה".
- המחרוזת IN מציינת רשומת אינטרנט.
- כל שם מארח שאינו מסתיים בנקודה (.) יצורף ל- Root Domain.
- הסימן @ מוחלף בסימן נקודה (.) בכתובת הדואר האלקטרוני של מנהל המערכת.
- סוגריים (()) חייבים לתחום מעברי שורה הפרושים על פני יותר משורה אחת.

רשומת שרת שמות

רשומת שרת השמות (NS) מציינת את שרתי השמות הנוספים. קובץ מסד נתונים יכול לכלול יותר מאשר רשומת NS יחידה. השורה הבאה היא דוגמה לרשומת NS:

```
@    IN    NS    nameserver2.microsoft.com
```

רשומת מארח

רשומת משאב כתובת מארח (A) משייכת באופן קבוע שם מארח עם כתובת ה-IP. רוב רובו של קובץ מסד הנתונים הוא רשומות מארח, והוא יכלול את כל המארחים באזור. השורות הבאות הן דוגמה לרשומות מארח:

```
rhino        IN   A    157.55.200.143
localhost    IN   A    127.0.0.1
```

רשומת CNAME

רשומת שם קאנוני (**C**anonical **Name**, CNAME) מאפשרת לך לשייך יותר משם מארח אחד לכתובת IP. לעיתים נקרא מצב כגון זה Aliasing. השורות הבאות הן דוגמה לרשומות CNAME:

```
FileServer1    CNAME    rhino
www            CNAME    rhino
ftp            CNAME    rhino
```

קובץ חיפוש לאחור

קובץ החיפוש לאחור (z.y.x.w.in-addr.arpa) מאפשר למיישב לספק כתובת IP ולבקש שם מארח תואם. קובץ חיפוש לאחור (Reverse Lookup File) נקרא כמו קובץ אזור, בהתאם לאזור in-addr.arpa בעבורו הוא מספק את החיפוש לאחור. לדוגמה, כדי לספק חיפוש לאחור לכתובת 157.57.28.0, נוצר קובץ חיפוש לאחור ששמו יהיה 57.157.in-addr.arpa. קובץ זה כולל רשומות SOA ו-NS דומות לקבצי אזור אחרים של DNS, וגם רשומות PTR.

אפשרות החיפוש לאחור זו היא חשובה, מפני שיישומים מסוימים מספקים את היכולת ליישום אבטחה מבוססת על התחברות לשמות מארחים. למשל, אם דפדפן שולח בקשה לשרת אינטרנט IIS (**I**nternet **I**nformation **S**erver) המוגדר לאפשרות אבטחה זו, יתקשר שרת האינטרנט עם שרת ה-DNS ויבצע שם חיפוש לאחור על כתובת ה-IP של הלקוח. אם

שם המארח שהוחזר על ידי שרת ה-DNS אינו ברשימת הגישה של אתר האינטרנט, או אם השם לא אותר על ידי שרת ה-DNS, אז הבקשה תידחה.

הערה Windows 2000 אינה דורשת הגדרת אזורי חיפוש לאחור. אזורי חיפוש לאחור (Reverse-Lookup Zones) עשויים להיות נדרשים ליישומים אחרים, או לנוחיות הניהול.

רשומת PTR

רשומות PTR מספקות מיפוי כתובת-לשם בתוך אזור חיפוש לאחור. מספרי IP נרשמים בסדר הפוך ולסופם מוצמדת המחרוזת in-addr.arpa, כדי ליצור את רשומת PTR זו. כדוגמה, חיפוש אחר השם עבור הכתובת 157.55.200.51 דורש שאילתת PTR אחר השם 51.200.55.157.in-addr.arpa. דוגמה לכך עשויה להיראות כך :

```
51.200.55.157.in-addr.arpa.     IN   PTR mailserver1.microsoft.com.
```

קובץ המטמון

הקובץ CACHE.DNS מכיל את הרשומות של שרתי Root Domain. קובץ המטמון הוא בעיקרון אותו הדבר בכל שרתי השמות, והימצאותו היא חובה. כאשר שרת השמות מקבל שאילתה מחוץ לאזור שלו, הוא מתחיל את תהליך ההסדרה בשרתי Root Domain הללו. רשומה לדוגמה עשויה להיראות כך :

```
.                      360000  IN     NS      A.ROOT-SERVERS.NET
A.ROOT-SERVERS.NET     360000  A              198.41.0.4
```

קובץ המטמון מכיל את מידע המארח הנדרש להסדרת שמות מחוץ ל- Domains בעלי הסמכות, וגם מכיל שמות וכתובות של שרתי שמות ברמת השורש. בקובץ ברירת המחדל המסופק עם שרת DNS של Windows 2000 יש את הרשומות הנוכחיות עבור כל שרתי השורש באינטרנט, והוא מאוחסן בתיקיה %SystemRoot%\System32\Dns. עבור התקנות שאינן מקושרות לאינטרנט יש להחליף קובץ זה באחד שיכיל את ה- Authoritative Domains (תחומים בעלי הסמכות) של שרתי השמות עבור שורש הרשת הפרטית.

קובץ האתחול

קובץ האתחול (Boot File) הוא קובץ ההגדרה הראשוני (Startup Configuration) ביישום DNS הייחודי של Berkeley Internet Name Deamon. קובץ זה מכיל מידע מארח הנדרש להסדרת שמות מחוץ ל- Authoritative Domains. הקובץ אינו מוגדר ב-RFC (**R**equest **F**or **C**omments) ואינו נדרש לשם תאימות-RFC. הוא נתמך על ידי Windows 2000 כדי לשפר תאימות עם שירותי DNS מבוססי-UNIX המוכרים. קובץ האתחול של Berkeley Internet Name Deamon שולט בתהליך ההגדרה הראשוני של שרת DNS. פקודות חייבות להתחיל בתחילת שורה ואסור שייקדם להן תו רווח. טבלה 7.1 מציגה תיאור של חלק מפקודות קובץ האתחול, הנתמכות על ידי Windows 2000.

טבלה 7.1 פקודות קובץ האתחול של Windows 2000

הפקודה	תיאור
Directory	הספריה בה ניתן למצוא קבצים אחרים אליהם יש התייחסות בקובץ האתחול.
Cache	מציינת קובץ המשמש לסייע לשירות DNS לתקשר עם שרתי שמות עבור ה- Root Domain. חובה לכלול פקודה זו ואת הקובץ אליה היא מתייחסת. Windows 2000 כוללת קובץ מטמון המתאים לשימוש באינטרנט.
Primary	מציינת את ה- Domain בו שרת שמות זה הוא בעל סמכות, וקובץ מסד נתונים אשר מכיל את רשומות המשאבים (RR) עבור Domain זה (כלומר, קובץ האזור - Zone File). קובץ אתחול אחד יכול לכלול מספר מרובה של רשומות פקודות מסוג זה.
Secondary	מציינת Domain בו שרת שמות זה הוא בעל סמכות ורשימת כתובות IP של Master Servers (שרתים ראשיים) מהם יש לנסות למשוך את מידע האזור, במקום לקרוא אותו מקובץ. היא גם מגדירה את השם של קובץ מקומי למיטמון אזור זה. קובץ אתחול אחד יכול לכלול מספר מרובה של רשומות פקודות מסוג זה.

טבלה 7.2 מציגה דוגמאות של הפקודות בקובץ האתחול.

טבלה 7.2 פקודות קובץ האתחול של Windows 2000

תחביר	דוגמה
directory [directory]	directory c:\winnt\system32\dns
cache.[file_name]	cache.cache
primary [domain] [file_name]	primary microsoft.com microsoft.dns primary dev.microsoft.com dev.dns
secondary [domain][hostlist][local_file_name]	secondary test.miccrosoft.com 157.55.200.100 test.dns

סיכום שיעור

כשלקוחות מבקשים להסדיר שם Host לכתובת IP, הם יכולים לבצע אחת משלוש שאילתות לשרתי DNS: רקורסיבית, איטרטיבית או אינברסית. כשהלקוח מבצע שאילתה רקורסיבית, יחזיר שרת DNS רק את המידע שקיים במטמון שלו, כולל האפשרות לשגיאה. שאילתה איטרטיבית היא שכיחה יותר. כשלקוח מבצע שאילתה איטרטיבית, יחזיר שרת ה-DNS את המידע המבוקש, או שיספק ללקוח כתובת של שרת DNS חילופי, שיספק את המידע המבוקש. שאילתה, אינברסית, מספקת מידע של חיפוש לאחור (Reverse Lookup). אם לקוח DNS צריך לתרגם כתובת IP ידועה לשם המארח, נשלחת לשרת ה-DNS שאילתה אינברסית.

שרתי DNS מאחסנים את מידע השמות וההגדרה שלהם בארבעה קבצים: מסד נתונים (Database), חיפוש לאחור (Reverse-Lookup), מטמון (Cache) ואתחול (Boot). Windows 2000 ומנהל DNS המצורף לה, DNS Manager, מאפשרים לך להגדיר את קבצים אלה באמצעות ממשק משתמש גרפי המתואר בפירוט בפרק 8.

שיעור 3: תכנון יישום DNS

הגדרת שרתי ה-DNS שלך תלויה בגורמים, כגון גודל הארגון שלך, מיקומם של משרדי הארגון ודרישות העמידות בפני תקלות (Fault Tolerance). שיעור זה יאיר בפניך את הדרך להגדרת DNS עבור האתר שלך. הוא מכיל תרחישים אשר יבחנו את ידיעותיך בתכנון רשת, קודם לביצוע ההתקנה הממשית של DNS.

לאחר שיעור זה, תוכל

- לרשום את שרת DNS שלך עם Parent Domain.
- להעריך את מספר שרתי שמות DNS, Domains ו-Zones הנדרשים לרשת.

זמן לימוד משוער: 40 דקות

שיקולים ב-DNS

למרות ש- Windows 2000 ונושא הסדרת השמות בה דורשים שרת DNS, שרת ה-DNS עצמו לא חייב להיות מותקן דווקא בשרת המפעיל את Windows 2000 Server. מעבר לכך, הוא כלל לא חייב להיות מותקן ברשת המקומית שלך. כל עוד ניתן להגדיר את Windows 2000 כך שתתייחס לשרת DNS חוקי התומך בסוג הרשומות הנדרש, כגון זה המותקן אצל ספק שירותי האינטרנט שלך, תוכל לספק את שירותי הסדרת השמות ל- Windows 2000. אבל, כאשר תבחן את הפונקציונליות המורחבת של גרסת DNS המצורפת ל- Windows 2000, ייתכן מאוד שתחליט שראוי להתקין ולהגדיר שרת DNS משל עצמך. לצורך מטרותיו של שיעור זה, מוגדרת נקודת הנחה שהחלטת ליישם שרת DNS משל עצמך.

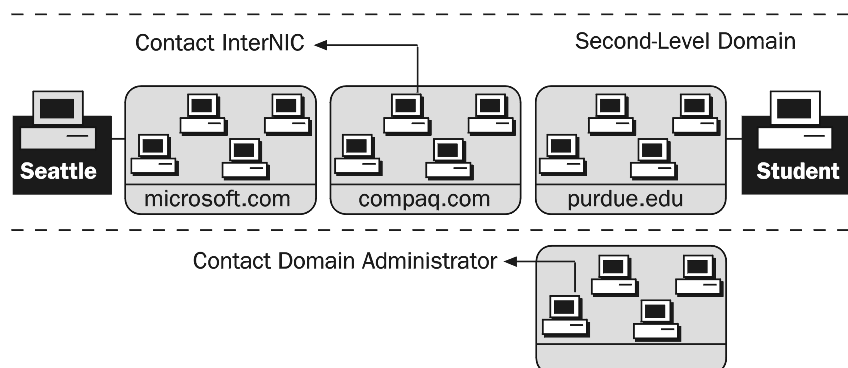
אם הארגון שלך, ואין זה משנה מה גודלו, מעוניין להשתמש ב-Domain ברמה משנית (Secondary-Level Domain), יש ליידע את InterNIC (**Inter**net **N**etwork **I**nformation **C**enter) לגבי שם ה-Domain של הארגון שלך, ולפחות שתי כתובות של שרתי DNS המשרתים את הארגון. תוכל להגדיר שרתי DNS נוספים בארגון, כאשר הם נפרדים מהאינטרנט.

מטעמי אמינות (Reliability) ויתירות (Redundancy), ממליצה Microsoft שיוגדרו לפחות שני שרתי DNS בארגון, שרת שמות עיקרי ושרת שמות משני. שרת השמות העיקרי מתחזק את מסד הנתונים, אשר משוכפל לשרת השמות המשני. שכפול זה מאפשר לשאילתות השמות להיות מבוצעות גם במידה ואחד מהשרתים אינו זמין. תזמון השכפול יכול להיות מוגדר בהתאם לחלופת השמות ב-Domain. שכפול אמור להתבצע לעיתים קרובות מספיק, כך שהשינויים יהיו ידועים לשני השרתים. אבל, שכפול עודף יכול להגדיל את תעבורת הרשת ולגרום לעומס מיותר על שרת השמות.

רישום Parent Domain

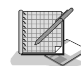
לאחר שהגדרת והתקנת את שרתי ה-DNS שלך, עליך לרשום (Register) אותם בשרת ה-DNS שברמה מעליך במבנה השמות ההיררכי של DNS. תרשים 7.5 מציג דוגמה לרישום שרת ה-DNS שלך ב-Domain ברמה מעליו. מערכת האב (Parent System) צריכה את

כתובות ושמות השרתים שלך ועשויה לדרוש גם מידע נוסף, כגון התאריך בו יהיה ה-Domain זמין ושמות וכתובות דיוור של אנשי הקשר המתחזקים אותו.



תרשים 7.5 רישום שרת ה-DNS שלך ל- Domain ברמה מעליו

אם אתה נרשם ב-Domain שהוא נמוך מהרמה המשנית, בדוק עם מנהל אותה המערכת איזה מידע אתה אמור לספק.



תרגול: יישום DNS

בתרגול זה תסקור שלושה תרחישים ליישום DNS. בכל אחד מתרחישים אלה עליך להעריך את מספר שרתי שמות DNS, ה-Domains וה-Zones הדרושים לרשת. כל תרחיש מתאר חברה המהגרת לסביבת Windows 2000 ומעוניינת גם ליישם את Directory Services. יהיה עליך לענות על מספר שאלות הקשורות בשרטוט טיוטה לתכנון רשת DNS עבור כל חברה, תוך שימוש בקריטריונים מיוחדים. מטרת תרגולים אלה היא לבחון את ידיעותיך בתכנון רשת קודם להתקנת DNS. הדבר ישרת כנקודת בסיס לבחינת רמת הידע שלך בסיום קורס זה, ויסייע לך להתחיל לחשוב אודות עיצוב ותכנון רשת DNS.

תרחיש 1: תכנון DNS עבור רשת קטנה

חברת Northwind נמצאת בתהליך החלפת מערכת המחשוב המיושנת שלה למערכת חדשה מבוססת Windows 2000. רוב העובדים מבצעים גישה למערכת המיושנת באמצעות מסופים. משתמשים אחדים משתמשים במערכות מבוססות מעבדי 486 ולחלקם מערכות מבוססות מעבדי פנטיום; מחשבים אלה אינם מחוברים לרשת. החברה כבר רכשה את הציוד הנדרש להגירה.

הרשת תשתמש בשיתוף קבצים והדפסה בסיסי, ויופעל בה שרת Windows 2000 אחד, בו יופעל גם שרת SQL גירסה 7 של Microsoft. רובם המכריע של המשתמשים יצטרך גישה למחשב בו פועל שרת ה-SQL. יישומי שולחן העבודה יותקנו בתחנות באופן מקומי, אך קבצי הנתונים יישמרו בשרתים.

חברת Northwind מעוניינת להיות מחוברת לאינטרנט, כדי שהעובדים יוכלו לקבל דואר אלקטרוני.

שרטט טיוטה לתכנון הרשת תוך שימוש בקריטריונים המוצגים בטבלה 7.3.

טבלה 7.3 קריטריונים לעיצוב רשת

רכיבים סביבתיים	פירוט
משתמשים	100
מיקומים	משרד יחיד
ניהול	מנהל מערכת אחד במשרה מלאה
שרתים	3 מחשבים: שני מחשבים מבוססי מעבד Pentium 120 בהם 32MB זיכרון RAM וכונן דיסק קשיח בנפח 3.2GB; מחשב אחד מבוסס מעבד Pentium 150 ובו 128MB זיכרון RAM המיועד עבור שרת Exchange.
לקוחות	כולם מבוססי מעבדי 486 או Pentium, מבוססי מערכת הפעלה Windows 2000 Professional.
יישומי BackOffice	שרת Exchange ו-DNS
שימושי השרת	קבצים והדפסה בסיסי

נקודות שצריך להתחשב בהן בעת תכנון הרשת:

- מספר המשתמשים
- מספר יחידות הניהול
- מספר האתרים

בהתבסס על מטרות התכנון, ענה על השאלות הבאות:

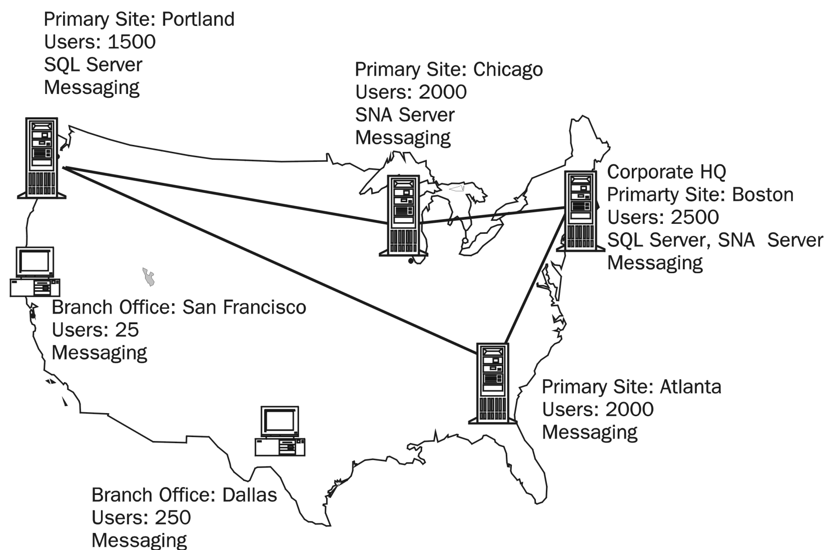
1. כמה Domains של DNS אתה צריך להגדיר?
2. כמה Subdomains אתה צריך להגדיר?
3. כמה Zones (אזורים) אתה צריך להגדיר?
4. כמה Primary Name Servers (שרתי שמות עיקריים) אתה צריך להגדיר?
5. כמה Secondary Name Servers (שרתי שמות משניים) אתה צריך להגדיר?
6. כמה שרתי DNS מטמון-בלבד (Cache-Only) אתה צריך להגדיר?

תרחיש 2: תכנון DNS עבור רשת בינונית

אתה יועץ לחברת Northwind, לה יש 8,795 משתמשים. קיימים 8,000 משתמשים הפרושים בארבעה אתרים עיקריים, ויתרת העובדים פזורים ב-10 סניפים בערים גדולות. החברה החליטה לשדרג את רשתות ה-LAN הקיימות שלה ל- Windows 2000 Server. עוד

הוחלט בארגון לרכז את כל חשבונות המשתמשים במיקום יחיד, במשרד הראשי של הארגון.

כפי שמתואר בתרשים 7.6, ארבעה האתרים העיקריים מחוברים ביניהם בקווי תקשורת בנפח T1. הסניפים מחוברים לאתר העיקרי הקרוב ביותר בקווי תקשורת בנפח 56Kbps.



תרשים 7.6 חיבורים למשרד הראשי

שלושה מבין ארבעה האתרים העיקריים הם יחידות עסקיות עצמאיות הפועלות בנפרד מהשאר. האתר הרביעי הוא המשרד הראשי (Corporate Headquarters). בסניפי החברה יש 25 עד 250 משתמשים הצריכים גישה לכל אחד מארבעת האתרים העיקריים, אך לעיתים רחוקות נמצא הצורך בגישה לסניף אחר.

בנוסף לעשרה הסניפים, גילית שלחברה יש אתר מחקר ופיתוח זמני, בו מועסקים 10 עובדים. באתר זה יש שרת יחיד המתחבר לבוסטון באמצעות נתבי חיוג-על-פי-דרישה (Dial-on-demand Routers). אתר זה צפוי להיסגר תוך שישה חודשים. אתר זה פועל כיחידה עצמאית ודורש חיבוריות לצרכי הודעות (Messaging) בלבד.

האתרים העיקריים ימשיכו לתחזק את הציוד שלהם ואת הציוד שבסניפים המחוברים אליהם. נכון לרגע זה, ניצולת רוחב הפס עומדת על 60 אחוז בשעות העומס. צמיחת הרשת אמורה להיות מזערית למשך 12 עד 18 החודשים הקרובים.

שרטט טיוטה לתכנון הרשת, תוך שימוש בקריטריונים המוצגים בטבלה 7.4.

טבלה 7.4 קריטריונים לתכנון רשת

רכיבים סביבתיים	פירוט
משתמשים	8,795
מיקומים	ארבעה אתרים עיקריים ו-10 סניפים בערים גדולות בארה"ב. אין בתכנון הקמת מיקומים בינלאומיים.
ניהול	מנהלי מערכת במשרה מלאה בכל אחד מהאתרים העיקריים, בחלק מהסניפים יועסק מנהל מערכת במשרה חלקית.
מספר שרתי שמות	יש לקבוע
מספר שרתי מטמון	יש להתקין שרתי מטמון DNS בכל אחד מהמיקומים המרוחקים באותו אזור.
לקוחות	מבוססי מעבדי 386, 486 ו-Pentium, מבוססי מערכת הפעלה Windows 2000 Professional.
יישומי שרת	שרת SQL 7.0, שרת Exchange ו-DNS

מספר המשתמשים בסניפים הוא: לוס אנג'לס, 40 משתמשים; סולט לייק סיטי, 25 משתמשים; מונטריאול, 30 משתמשים; ניו אורלינס, 25 משתמשים; קנזס סיטי, 25 משתמשים; וושינגטון הבירה, 100 משתמשים; דנבר, 250 משתמשים; מיאמי, 75 משתמשים.

נקודות שצריך להתחשב בהן בעת תכנון הרשת:

- מספר המשתמשים
- מספר יחידות הניהול (Administrative Units)
- מספר האתרים
- מהירות ואיכות הקישורים המחברים בין האתרים
- רוחב פס זמין בקישורים
- שינויים צפויים ברשת
- יישומים עסקיים

בהתבסס על מטרות התכנון, ענה על השאלות הבאות:

1. כמה תחומי DNS אתה צריך להגדיר?
2. כמה Subdomains אתה צריך להגדיר?
3. כמה Zones אתה צריך להגדיר?
4. כמה שרתי שמות עיקריים אתה צריך להגדיר?
5. כמה שרתי שמות משניים אתה צריך להגדיר?
6. כמה שרתי DNS מטמון-בלבד (Cache-Only) אתה צריך להגדיר?

7. היעזר בטבלת המרחקים הבאה כדי לתכנן תצורת אזור/סניף, בהתבסס על סמיכות גיאוגרפית בין כל אתר עיקרי וסניף. סניפים צריכים להיות באותו אזור של האתר העיקרי הקרוב ביותר.

אזורים (Zones) לכל סניף (בהתבסס על סמיכות גיאוגרפית):

טבלת מרחקים	אטלנטה	בוסטון	שיקאגו	פורטלנד
דאלאס	807	1817	934	2110
דנבר	1400	1987	1014	1300
וושינגטון הבירה	632	435	685	2700
לוס אנג'לס	2195	3050	2093	1143
מונטריאול	1232	322	846	2695
מיאמי	665	1540	1358	3300
ניו אורלינס	494	1534	927	2508
סולט לייק סיטי	1902	2403	1429	800
סן פרנסיסקו	2525	3162	2187	700
קנזס סיטי	809	1454	497	1800

תרחיש 3: תכנון DNS עבור רשת גדולה

לחברת Northwind יש 60,000 משתמשים הממוקמים בכל רחבי העולם. המשרד הראשי של החברה ממוקם בג'נבה, שוויצריה. המשרד הראשי לצפון ולדרום ארה"ב ממוקם בעיר ניו יורק. המשרד הראשי של אוסטרליה ואסיה ממוקם בסינגפור. בכל אחד מהמשרדים האזוריים הראשיים תתבצע תחזוקה ושליטה מלאה במשתמשים באזורם. למשתמשים נדרשת גישה למשאבים במשרדים האזוריים הראשיים האחרים. שלושת המשרדים האזוריים הראשיים מחוברים ביניהם בקווי תקשורת בנפח T1.

לכל אחד משלושת המשרדים האזוריים הראשיים יש יישומים עיסקיים אשר צריכים להיות זמינים לכל האתרים באזורם, כמו גם למשרדים האזוריים הראשיים האחרים. לחברות הבת שבמלזיה ובאוסטרליה יש אתרי ייצור גדולים, אליהם צריכה להיות גישה לכל חברות הבת האזוריות.

יישומים עסקיים אלה פועלים בסביבת שרתים מבוססי Windows 2000. מחשבים אלה יוגדרו כשרתים בתוך התחומים. הקישורים בין סינגפור, אוסטרליה ומלזיה פועלים בדרך כלל בניצולת של 90 אחוז. אזור אסיה ואוסטרליה כולל 10 חברות בת, הכוללות את אוסטרליה, סין, אינדונזיה, יפן, קוריאה, מלזיה, ניו זילנד, סינגפור, טאיוון ותאילנד.

בשל הגבלות הייבוא החלות על חלק מחברות הבת הוחלט שכל חברה בת תקבל את השליטה בציוד המותקן בה, ולמקם Resource Domain בכל חברת בת. לאחרונה, רוב המחשבים שנרכשו על ידי חברות הבת פועלים בסביבת מערכת ההפעלה Windows 2000 Professional. החברה אישרה יתירות חומרה במקרים בהם ניתן להצדיק זאת.

כדי לשמור על סבירות תרחיש זה, השאלות והתשובות קשורות רק לאזור אסיה ואוסטרליה.

שרטט טיוטה לתכנון הרשת, תוך שימוש בקריטריונים המוצגים בטבלה 7.5.

טבלה 7.5 קריטריונים לתכנון רשת

רכיבים סביבתיים	פירוט
משתמשים ב-Domain אסיה ואוסטרליה	25,000 פזורים באופן שווה בין כל חברות הבת.
מיקומים	משרד ראשי אזורי ממוקם בסינגפור; 10 חברות בת באוסטרליה, סין, אינדונזיה, יפן, קוריאה, מלזיה, ניו זילנד, סינגפור, טאיוון ותאילנד.
ניהול	מנהלי מערכת במשרה מלאה במשרד האזורי הראשי ובכל אחת מחברות הבת.
מספר ה-Domains	יש לקבוע
לקוחות	מבוססי מעבדי 386, 486 ו-Pentium, מבוססי מערכת הפעלה Windows 2000 Professional.
יישומי שרת	שרת SQL 7.0, שרת SNA, שרת SMS (**S**ystem **M**anagement **S**erver), Messaging ו-DNS
מספר שרתי מטמון	יש לקבוע

נקודות שצריך להתחשב בהן בעת תכנון הרשת באזור אסיה ואוסטרליה:

- מספר המשתמשים
- מספר יחידות הניהול
- מספר האתרים
- מהירות ואיכות הקישורים המחברים בין האתרים
- רוחב פס זמין בקישורים
- שינויים צפויים ברשת
- יישומים עסקיים

בהתבסס על מטרות התכנון, ענה על השאלות הבאות:

1. כמה תחומי DNS אתה צריך להגדיר?
2. כמה Subdomains אתה צריך להגדיר?
3. כמה Zones אתה צריך להגדיר?
4. כמה שרתי שמות עיקריים אתה צריך להגדיר?

5. כמה שרתי שמות משניים אתה צריך להגדיר?
6. כמה שרתי DNS מטמון-בלבד (Cache-Only) אתה צריך להגדיר?

סיכום שיעור

בהתאם לגודל הארגון ותצורתו, ייתכן שתרצה להגדיר DNS עבור האתר שלך. Windows 2000 דורשת גישה לשרת DNS כדי לספק פונקציונליות מלאה. שרת DNS זה יכול להיות מותקן ברשת המקומית שלך, או להיות מסופק מרחוק, על ידי ספק שירותי האינטרנט (ISP) שלך. אבל, יישום DNS הנכלל במערכת ההפעלה Windows 2000 כולל מספר תכונות נוספות מעבר לשרתי DNS הרגילים. למידע נוסף אודות תכונות חדשות אלו, קרא את פרק 8.

שיעור 4: התקנת DNS

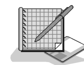
Microsoft DNS הוא שרת DNS תואם RFC; כתוצאה מכך, הוא יוצר ומשתמש בקבצי אזור DNS סטנדרטיים, ותומך בכל סוגי רשומות המשאבים (RR) הסטנדרטיים. הוא מאפשר פעולה משולבת עם שרתי DNS אחרים וכולל כלי אבחון DNS בשם NSLOOKUP. Microsoft DNS מהווה חלק אינטגרלי של Windows Internet Name Service (WINS) ומנוהל באמצעות תוכנית ניהול גרפית בשם DNS Manager. בשיעור זה תתקין את שירות DNS ב-Windows 2000.

לאחר שיעור זה, תוכל

- להתקין את שירות Microsoft DNS Server.
- לאתר ולטפל בתקלות DNS באמצעות NSLOOKUP.

זמן לימוד משוער: 45 דקות

לפני התקנת השירות Microsoft Windows 2000 DNS Server חשוב מאוד שפרוטוקול TCP/IP יהיה מותקן ומוגדר כהלכה בשרת Windows 2000. שירות DNS Server משיג את הגדרות ברירת המחדל עבור שם מארח ושם ה- Domain מתוך תיבת הדו-שיח Microsoft TCP/IP Properties. שירות DNS Server ייצור ברירת מחדל של רשומות SOA, מארח ו-NS, בהתבסס על שם ה- Domain ושם המארח המצויינים. אם לא צוינו שם ה-domain ושם מארח, נוצרת רק רשומת SOA.

 תרגול: התקנת שירות שרת DNS

בתרגול זה תתקין את שירות Microsoft DNS Server. את הגדרות ה-DNS תבצע בשיעור מתקדם יותר.



לפני שתמשיך עם שיעור זה, הפעל את קובץ ההדגמה Ch07a.exe שבתיקיה Media בתקליטור המצורף לספר זה. הקובץ מספק סקירה כללית לגבי התקנת שירות השרת של DNS.

הערה השלם הליך זה במחשב אותו אתה מייעד להיות שרת DNS.

לפני הגדרת DNS, ודא שהגדרות ה-DNS בלקוח נכונות.

➢ **כדי לוודא את הגדרות ה-DNS בלקוח**

1. לחץ לחיצה ימנית על הסמל My Network Places, ומתפריט הקיצור בחר Properties.

   מופיעה תיבת דו-שיח Network and Dial-up Connections.

2. לחץ לחיצה ימנית על חיבור הרשת (בדרך כלל זהו Local Area Connection) עבורו אתה מעוניין להגדיר את שרת ה-DNS, ומתפריט הקיצור בחר Properties.

   מופיעה תיבת דו-שיח Properties עבור החיבור המבוקש.

3. לחץ על Internet Protocol (TCP/IP), ולחץ Properties.

מופיעה תיבת דו-שיח Internet Protocol (TCP/IP) Properties.

4. בתיבת דו-שיח Internet Protocol (TCP/IP) Properties, בתיבה Preferred DNS Server הקלד את כתובת ה-IP של שרת DNS קיים.

תוכל להוסיף את כתובתו של שרת DNS חילופי, בתיבה Alternate DNS Server.

5. אם עליך להגדיר יותר מאשר שרת DNS חילופי אחד, לחץ על Advanced, בחר בכרטיסיה DNS, והקלד את כתובות השרתים בתיבה DNS Server Addresses.

6. לחץ OK כדי לסגור את תיבת דו-שיח Internet Protocol (TCP/IP) Properties.

7. לחץ OK כדי לסגור את תיבת דו-שיח Properties עבור החיבור.

➢ כדי להתקין את שירות DNS Server

1. בלוח הבקרה לחץ לחיצה כפולה על Add/Remove Programs, ולחץ על Add/Remove Windows Components.

מופיע חלון של Windows Components Wizard.

2. לחץ על Networking Services, ולחץ על Details.

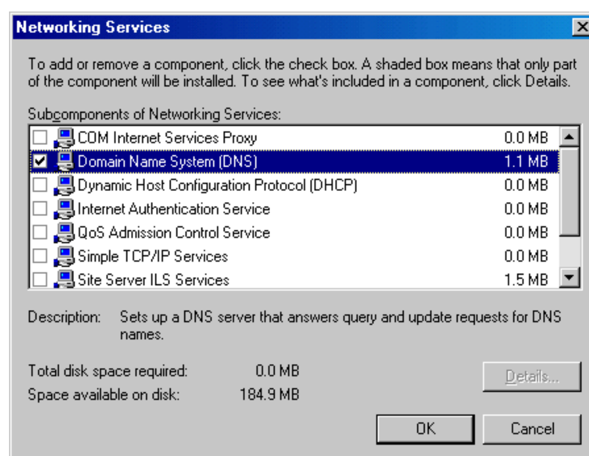
מופיעה תיבת דו-שיח Networking Services.

3. אם עדיין אינו נבחר, סמן את תיבת הסימון שליד **D**omain **N**ame **S**ystem (DNS), כפי שנראה בתרשים 7.7, ולחץ OK.

4. לחץ Next.

Windows 2000 מתקינה את DNS.

5. לחץ Finish.



תרשים 7.7 תיבת הסימון Domain Name System (DNS) בחלון Networking Services

איתור וטיפול בתקלות DNS באמצעות NSLOOKUP

NSLOOKUP הוא כלי שירות יעיל לאיתור וטיפול בתקלות DNS, כגון הסדרת שמות מארחים. כשאתה מפעיל את NSLOOKUP הוא מציג את שם המארח וכתובת ה-IP של שרת ה-DNS המוגדר עבור המערכת המקומית, ואז מציג מנחה שורת פקודה, לביצוע שאילתות נוספות. אם תקיש סימן שאלה (?/) יציג NSLOOKUP את כל הפקודות הזמינות. אתה יכול לצאת מהתוכנית על ידי הקלדת הפקודה exit. כדי לחפש כתובת IP של מארח תוך שימוש ב-DNS, הקלד את שם המארח והקש Enter. ברירות המחדל של NSLOOKUP לשימוש בשרת DNS מוגדרות עבור המחשב בו מופעלת תוכנית השירות, אך תוכל למקד אותה בשרת DNS אחר על ידי הקלדת הפקודה server <name> (כאשר <name> הוא שם המארח של השרת בו אתה מעוניין להשתמש לצורך חיפושים בעתיד). לאחר שהוגדר שרת אחר, כל מה שיוקלד מנקודה זו ואילך ייחשב כשם מארח.

מצבי NSLOOKUP

ל- NSLOOKUP יש שני מצבי עבודה: אינטראקטיבי ולא-אינטראקטיבי. אם נדרשת פיסת מידע יחידה, השתמש במצב הלא-אינטראקטיבי או במצב מנחה שורת הפקודה. אם יותר מפיסת מידע אחת נחוצה, ניתן להשתמש במצב האינטראקטיבי.

תחביר NSLOOKUP

NSLOOKUP.EXE הוא כלי ניהול של שורת הפקודה שנועד לניסוי ואבחון תקלות בשרתי DNS. התחביר הבא משמש להפעלת תוכנית השירות NSLOOKUP:

nslookup [-option...] [computer-to-find] - [server]

תחביר	תיאור
[-option ...]	מציין את אחת או יותר מפקודות NSLOOKUP. לקבלת רשימת הפקודות הזמינות היעזר באפשרות העזרה המובנית של NSLOOKUP
computer-to-find	אם ערך computer-to-find הוא כתובת IP, וסוג השאילתה הוא מארח או PTR, מוחזר שם המחשב. אם comuter-to-find הוא שם שאינו מסתיים בנקודה, מצורף לשם זה גם שם domain ברירת המחדל. כדי לאתר מחשב מחוץ ל- Domain הנוכחי הוסף נקודה בסוף השם. אם במקום computer-to-find מוקלד התו מקף (-), משתנה מצב ההפעלה של NSLOOKUP למצב אינטראקטיבי.
server	השתמש בשרת זה כשרת שמות. אם פרמטר זה אינו קיים, ייעשה שימוש בשרת DNS המוגדר כברירת מחדל.

➤ כדי להשתמש ב-NSLOOKUP במצב פקודה

1. בשורת פקודה שנה את המאפיינים, כך שערך מאגר (Buffer) חלון שורת הפקודה (Command Prompt) יהיה 50.

   כפי שמודגם בתרשים 7.8, היעזר לצורך כך בכרטיסיה Layout. אתה אמור להיות מסוגל לבצע פעולה זו כך שתשפיע על כל המופעים העתידיים של חלון שורת הפקודה; הדבר יידרש בשיעורים מתקדמים יותר.

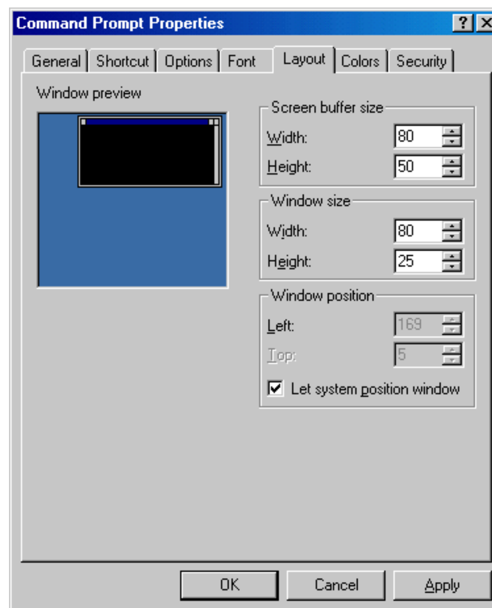
2. הקלד את הפקודה הבאה:

nslookup hostx

כאשר hostx הוא מארח ב- Domain שלך.

3. NSLOOKUP יחזיר את כתובת ה-IP של המחשב hostx, מפני שנתון זה מאוחסן במסד הנתונים של DNS.

4. צא מחלון שורת הפקודה.



תרשים 7.8 תיבת דו-שיח Command Prompt Properties

➢ כדי להשתמש ב-NSLOOKUP במצב אינטראקטיבי

1. במנחה שורת הפקודה הקלד nslookup, והקש Enter.

   מופיע המנחה <.

2. במנחה < הקלד את הפקודה set all, והקש Enter.

   פקודה זו מציגה את כל הערכים הנוכחיים של אפשרויות NSLOOKUP השונות.

3. השתמש בפקודות set הבאות כדי לשנות את ערך פסק-הזמן לשנייה אחת ואת מספר הניסיונות החוזרים ל-7, כפי שניתן לראות בתרשים 7.9.

```
Set ti=1
Set ret=7
```

4. השתמש בפקודה set all כדי לבחון שערכי ברירת המחדל אכן השתנו.

5. במנחה > הקלד את שמותיהם של המחשבים האחרים, אחד אחרי השני. הקש Enter לאחר כל שם.
6. צא מחלון שורת הפקודה.

```
Command Prompt
Default Server:  proxy1.rdc1.az.home.com
Address:  24.1.240.33

Set options:
  nodebug
  defname
  search
  recurse
  nod2
  novc
  noignoretc
  port=53
  type=A
  class=IN
  timeout=2
  retry=1
  root=A.ROOT-SERVERS.NET.
  domain=trainingassociates.com
  MSxfr
  IXFRversion=1
  srchlist=trainingassociates.com

> set ti=1
> set ret=7
>
```

תרשים 7.9 הגדרת ערך פסק הזמן ומספר הניסיונות החוזרים ב-NSLOOKUP

סיכום שיעור

DNS של Microsoft יכול לשתף פעולה עם שרתי DNS אחרים. לפני התקנת שירות DNS Server, עליך לוודא שפרוטוקול TCP/IP בשרת מוגדר כראוי.

תוכנית השירות NSLOOKUP היא כלי האבחון העיקרי עבור DNS. היא מאפשרת לך להציג רשומות משאבים בשרתי DNS.

שיעור 5: הגדרת DNS

קיימות שתי דרכים לנהל שרת DNS של Microsoft: להשתמש ב- DNS Manager או לערוך באופן ידני את קבצי התצורה של DNS. שיעור זה סוקר את הכלים לניהול שרת DNS.

לאחר שיעור זה, תוכל

- לנהל שרת DNS.
- ליצור קובץ אזור ולאכלס בו רשומות משאבים.

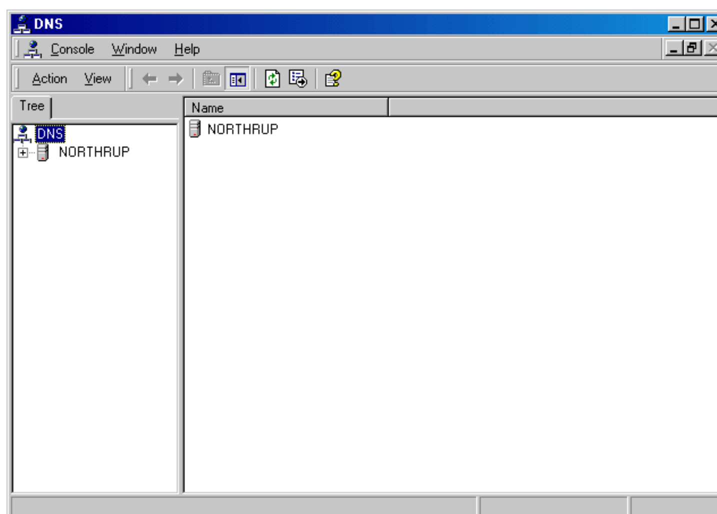
זמן לימוד משוער: 60 דקות

הגדרת מאפייני שרת DNS

כלי הניהול העיקרי בו תשתמש לניהול שרת DNS בסביבת Windows 2000 הוא הכלי DNS Manager, המתואר בתרשים 7.10. מכיון ששרת DNS אינו מכיל נתונים ראשוניים אודות משתמשי הרשת, מותקן שרת ה-DNS כשרת שמות מטמון-בלבד (Caching-Only Name Server) עבור האינטרנט. כלומר, שרת ה-DNS מכיל מידע לגבי שרתי השורש של האינטרנט בלבד. ברוב המקרים, הגדרת תצורת שרת DNS מחייבת אספקת נתונים נוספים, כדי שהוא יוכל לבצע את תפקידו המיועד.

➢ **כדי לפתוח DNS**

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ובחר DNS.



תרשים 7.10 הגדרות DNS ב-MMC

➢ כדי להגדיר שרת DNS חדש

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ובחר DNS.
2. סמן את השרת שלך. פתח את תפריט Action, ובחר Configure the Server.
3. עקוב אחר ההוראות שבאשף Configure DNS Server. באמצעות האשף תוכל ליצור אזור חיפוש לפנים (Forward Lookup Zone) אחד או יותר.

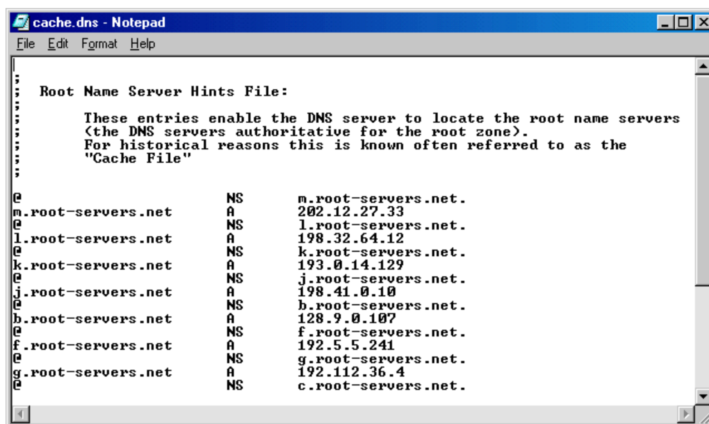
   סוג האזור שתוכל ליצור יכול להיות:

   - **Active Directory-Integrated.** DNS המשולב ב- Active Directory מאפשר אחסון ב- Active Directory ושכפול מסדי נתונים של אזורי DNS. נתוני האזור מאוחסנים כאובייקט Active Directory ומשוכפלים כחלק משכפול (Replication) ה- Domain.
   - **Standard Primary.** אזורים סטנדרטיים עיקריים דרושים כדי ליצור ולנהל אזורים במרחב שמות DNS (DNS Name Space) שלך, אם אינך משתמש ב- Active Directory.
   - **Standard Secondary.** אזורים סטנדרטיים משניים מסייעים לאזן את עומסי העיבוד בשרתים עיקריים, ומספקים סבילות בפני תקלות.

4. הצעד הבא באשף New Zone Wizard הוא ליצור אזור חיפוש קדימה או אחורה. אם תבחר באפשרות Forward Lookup Zone, עליך לספק שם עבור האזור החדש ואז לציין שם קובץ אזור. אם תבחר באפשרות Reverse Lookup Zone, עליך לספק מזהה רשת (Network ID) או שם אזור, ואז לציין קובץ אזור.
5. לחץ Finish כדי לסגור את האשף.

הגדרה ידנית של DNS

ניתן להגדיר שרת DNS באופן ידני, על ידי עריכת הקבצים המותקנים בתיקיית ברירת המחדל להתקנה, SystemRoot%\System32\Dns%. ניהול זה זהה לניהול DNS הקודם. קבצים אלה ניתנים לעריכה באמצעות כל עורך טקסט פשוט, כגון Notepad, כפי שניתן לראות בתרשים 7.11. כדי להכניס לתוקף את השינויים שביצעת, יש לעצור (Stop) את שירות DNS ולהפעילו מחדש (Restart).



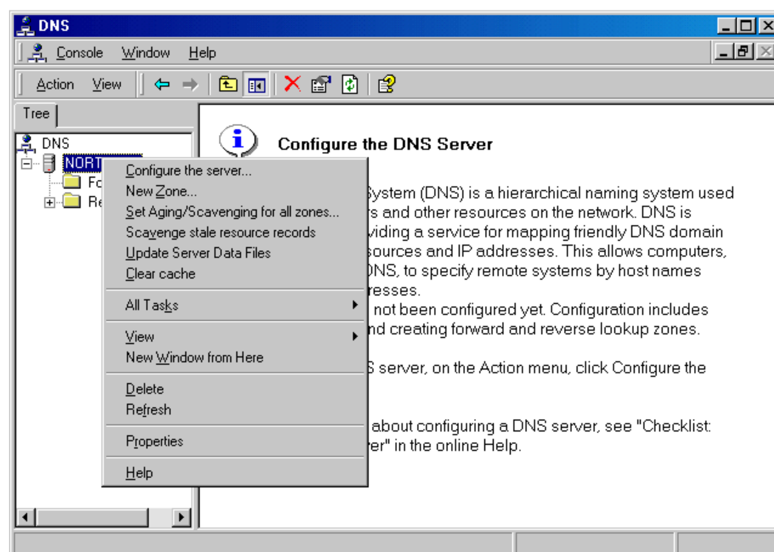
תרשים 7.11
עריכת הקובץ
CACHE.DNS

הוספת תחומי DNS ואזורי DNS

הצעד הראשון בהגדרת שרת DNS הוא לקבוע את ההיררכיה של תחומי ואזורי ה-DNS שלך. לאחר שנקבעו הנתונים לגבי ה-Domain והאזור יש להזין נתונים אלה לתצורת DNS תוך שימוש ב- DNS Console.

הוספת אזור עיקרי או אזור משני

אתה מוסיף אזור עיקרי או אזור משני באמצעות DNS Console, כפי שניתן לראות בתרשים 7.12. לאחר שהקלדת את נתוני האזור שלך, יבנה DNS Manager שם קובץ אזור של ברירת מחדל. אם קובץ האזור כבר קיים בתיקיית ה-DNS, MMC ייבא באופן אוטומטי את הרשומות מקובץ זה.



תרשים 7.12 יצירת אזור חדש באמצעות DNS Console

אזור עיקרי (Primary Zone) מאחסן את מיפויי שם-לכתובת באופן מקומי. כשאתה מגדיר אזור עיקרי, אינך זקוק למידע נוסף חוץ משם האזור.

אזורים משניים (Secondary Zone) מקבלים את מיפויי שם-לכתובת משרת ראשי (Master Server) על ידי העברת אזור (Zone Transfer). כאשר אתה מגדיר אזור משני עליך לספק את שם האזור ואת שרת השמות הראשי.

לאחר שכל ה- Zones נוספו לשרת, ניתן להוסיף Subdomains מתחת ל- Zones אלה. אם יש צורך במספר רמות של Subdomains, צור את ה- Subdomains בזה אחר זה. עבור כל אזור בעבורו יהיה ה-DNS בעל סמכות, נרשם מפתח (Key) ברישום המערכת (System Registry). את המפתחות תוכל למצוא תחת:

HKEY_CURRENT_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Zones

לכל אזור יש מפתח משלו המכיל את שם קובץ מסד הנתונים, מה שמציין האם שרת ה-DNS הוא שרת שמות עיקרי או משני. למשל, רשומת רישום המערכת הבאה נוצרת עבור האזור ששמו dev.volcano.com:

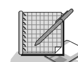
HKEY_CURRENT_MACHINE\SYSTEM\CurrentControlSet\
↳ Services\DNS\Zones\dev.volcano.com

הגדרת מאפייני אזור

לאחר שהוספת אזור בהצלחה, תוכל להגדיר ולשנות את מאפייני האזור (מתוארים בטבלה 7.6).

טבלה 7.6 מאפייני אזור

מאפיין	תיאור
General	מגדיר את קובץ האזור בו מאוחסנות רשומות המשאבים (RR) ומציין אם זהו שרת שמות עיקרי או משני.
SOA record	מגדיר מידע העברת אזור ואת תיבת הדואר של מנהל שרת השמות.
Notify	מציין את השרתים המשניים שאמורים להיות מיודעים כאשר משתנה מסד הנתונים בשרת העיקרי. בנוסף, ניתן להחיל אבטחה נוספת על שרת השמות על ידי הגדרה שרק שרתים משניים מסוימים יכולים לתקשר עם שרת זה.
WINS lookup	מאפשר לשרת השמות לבצע שאילתת WINS לצורך הסדרת שמות. בתיבת דו-שיח זו ניתן להגדיר רשימה של שרתי WINS. את שרתי ה-WINS ניתן לקבוע על בסיס שם שרת, על ידי סימון תיבת הסימון Settings Only Affect Local Server. אם אפשרות זו אינה מסומנת, ישתמשו גם השרתים המשניים בשרתי WINS המוגדרים כאן.



תרגול: התקנת שירות שרת DNS

בתרגול זה תגדיר את שרת ה-DNS, על ידי הוספת אזור עיקרי. השלם הליך זה במחשב המשמש כשרת DNS.



לפני שתמשיך עם שיעור זה, הפעל את קובץ ההדגמה Ch07b.exe שבתיקיה Media בתקליטור המצורף לספר זה. הקובץ מספק סקירה לגבי הגדרת שירות השרת של DNS.

➤ **כדי להוסיף אזור לשרת**

1. לחץ לחיצה ימנית על שם המחשב שלך ומתפריט הקיצור בחר New Zone.

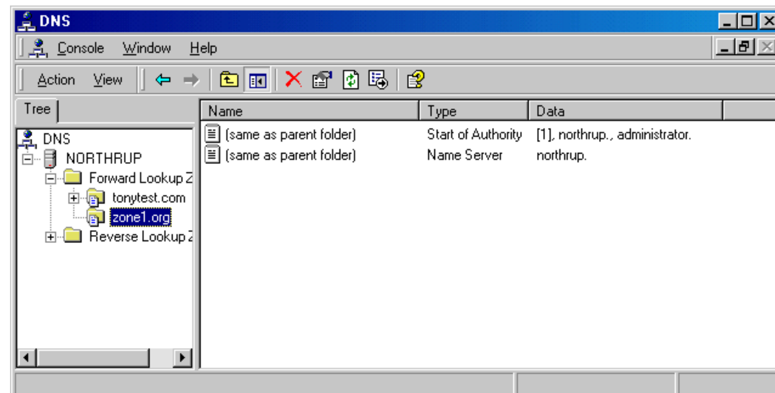
   מופיע האשף New Zone Wizard.
2. לחץ Next, בחר Standard Primary, ולחץ Next שוב.
3. בחר Forward Lookup Zone, ולחץ Next.
4. בתיבה Name הקלד zone1.org (כאשר zone1.org הוא שם האזור שלך).

5. סמן את Create a new file with this file name, ולחץ Next.

שם הקובץ יהיה Zone1.org.dns (כאשר zone1.org הוא שם האזור שלך).

6. לחץ על Finish כדי ליצור את האזור החדש.

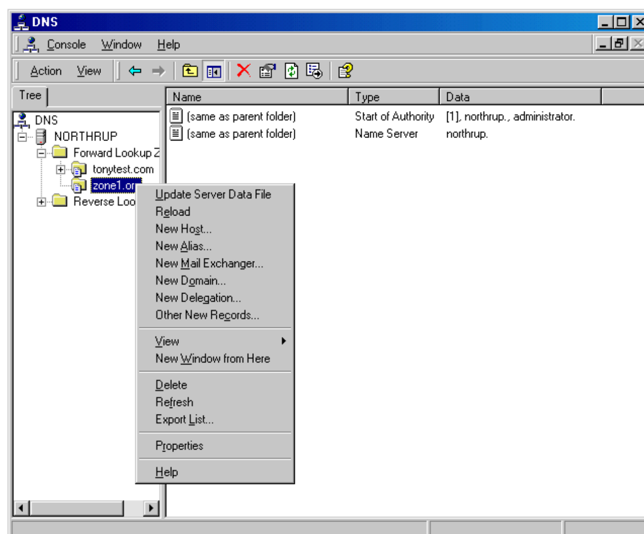
כעת מכילה התיקיה Forward Lookup Zone את האזור החדש שלך, כפי שניתן לראות בתרשים 7.13.



תרשים 7.13 אזור שנוסף לתיקיה Forward Lookup Zone

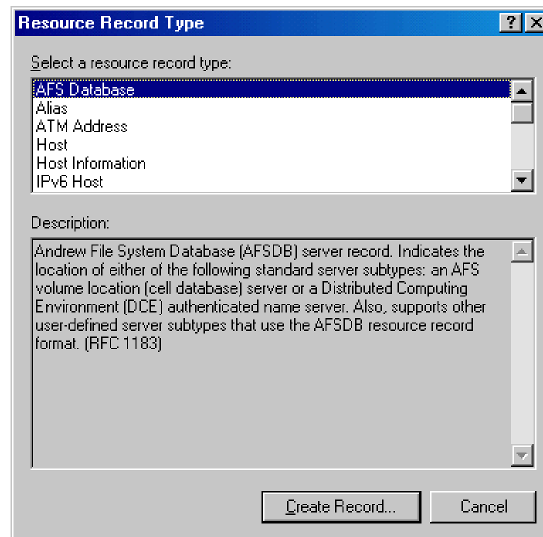
הוספת רשומות משאבים

לאחר שהוגדרו Zones ו- Subdomains, ניתן להוסיף רשומות משאבים (RR). כדי ליצור מארח חדש, לחץ לחיצה ימנית על האזור או ה-Subdomain ומתפריט הקיצור בחר New Host, כפי שניתן לראות בתרשים 7.14. הקלד את שם המארח, לחץ על Add Host ורשומות המארח תיווצר.



תרשים 7.14
הוספת מארח חדש

כדי ליצור רשומה מסוג אחר, לחץ לחיצה ימנית על האזור או ה- Subdomain ומתפריט הקיצור בחר Other New Record. כעת, בחר איזה סוג רשומת משאבים ליצור. תיבת דו-שיח מציגה מספר שדות הייחודיים לסוגי רשימות, כפי שניתן לראות בתרשים 7.15.



תרשים 7.15 בחירת סוג רשומה אותה יש ליצור

הגדרת חיפוש לאחור

כדי לאתר שם מארח, על ידי הצגת כתובת ה-IP שלו, יש ליצור אזור חיפוש לאחור (Reverse Lookup Zone) עבור כל רשת בה קיימים מארחים המופיעים במסד הנתונים של ה-DNS. אופן הוספת אזור חיפוש לאחור זהה לאופן הוספת כל סוג אחר של אזור, כאשר ההבדל היחידי הוא שם האזור. לדוגמה, אם למארח מוגדרת כתובת ה-IP 198.231.25.89, תהיה כתובת זו מיוצגת ב- in-addr.arpa Domain כ- 89.25.231.198.in-addr.arpa. יתר על כן, כדי לאפשר את הופעת מארח זה ללקוח לו יש את כתובת ה-IP שלו, יש צורך להוסיף ל-DNS אזור עבור 25.231.198.in-addr.arpa. כל רשומות PTR של הרשת 198.231.25.0 יוספו לאזור חיפוש לאחור זה.

סיכום שיעור

הצעד הראשון בהגדרת שרת DNS של Windows 2000 הוא לקבוע את ההיררכיה של תחומי ואזורי ה-DNS שלך. לאחר שהוגדרו ה- Zones וה- Subdomains ניתן להוסיף להם את רשומות המשאבים. כדי לאתר שם מארח, על ידי הצגת כתובת ה-IP שלו, יש ליצור אזור חיפוש לאחור (Reverse Lookup Zone) עבור כל רשת בה קיימים מארחים המופיעים במסד הנתונים של ה-DNS.

שאלות סיכום

השאלות הבאות נועדו לחזק את הנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות על שאלה, עיין בשיעור המתאים ונסה את השאלה שנית. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואחר כך בעברית.

Answering the following questions will reinforce key information presented in this chapter. If you are unable to answer a question, review the appropriate lesson and then try the question again. Answers to the questions can be found in Appendix A, "Questions and Answers".

1. Name the three components of the DNS.
2. Describe the difference between primary, secondary, and master name servers.
3. List three reasons to have a secondary name server.
4. Describe the difference between a domain and a zone.
5. Describe the difference between recursive and iterative queries.
6. List the files required for a Windows 2000 DNS implementation.
7. Describe the purpose of the boot file.

1. מנה את שלושת המרכיבים של DNS.
2. תאר את ההבדל בין שרת שמות עיקרי, משני וראשי.
3. מנה שלוש סיבות להגדרת שרת שמות משני.
4. תאר את ההבדל בין Domain לאזור (Zone).
5. תאר את ההבדל בין שאילתה רקורסיבית לשאילתה איטרטיבית.
6. מנה את הקבצים הנדרשים לצורך יישום DNS.
7. תאר את מטרתו של קובץ האתחול (Boot File).

פרק 8

שימוש ב-DNS בסביבת Windows 2000

אודות פרק זה

בפרק זה תלמד כיצד לעבוד עם אזורי DNS (**D**omain **N**ame **S**ystem). הנושא כולל יישום אזור מואצל (Delegated Zone) והגדרת אזורים לעדכונים דינמיים. בנוסף תלמד כיצד להגדיר שרת DNS שיפעל כשרת מטמון-בלבד, וכיתד לנטר את ביצועי שרת DNS.

לפני שתתחיל

להשלמת פרק זה צריך שיהיה ברשותך:

- ❖ מחשב בו מותקנת מערכת ההפעלה Windows 2000 Server, בה מוגדר פרוטוקול TCP/IP ומותקנים שירותי DNS.

שיעור 1: עבודה עם אזורים

שרתים פונים לאזורים שלהם (נקראים גם קבצי מסד נתוני DNS, DNS Database Files) לצורך הסדרת שמות. האזורים מכילים רשומות משאבים הבנויות מנתוני המשאב, כפי שהם משויכים ל-DNS Domain. לדוגמה, רשומות משאבים אחדות ממפות שמות ידידותיים לכתובות IP, וחלק אחר שלהן ממפות כתובות IP לשמות ידידותיים. רשומות משאבים מסוימות כוללות לא רק מידע אודות שרתים ב-DNS Domains, אלא גם משמשות להגדרת ה-Domain על ידי ציון לאיזה שרתים יש את הסמכות באיזה אזורים. בשיעור זה תלמד כיצד להגדיר אזורי DNS בסביבת Windows 2000.

לאחר שיעור זה, תוכל

- ליישם אזור מואצל (Delegated Zone) עבור DNS.
- להגדיר אזורים לעדכון דינמי.

זמן לימוד משוער: 20 דקות

אזורים מאצילים

מסד נתוני DNS יכול להיות מחולק (Partitioned) למספר אזורים. אזור (Zone) הוא חלק במסד נתוני DNS המכיל את רשומות המשאבים עם שמות הבעלים השייכים לחלק הרציף של מרחב השמות של DNS. קבצי אזור (Zone Files) מוחזקים בשרתי DNS. שרת DNS יחיד יכול להיות מוגדר שלא לכלול אף אזור, לכלול אזור יחיד או מספר רב של אזורים. כל אזור מעוגן לשם domain מסוים, אליו מתייחסים כאל Zone's Root Domain. אזור מכיל מידע אודות כל השמות המסתיימים בשמו של Zone's Root Domain. שרת DNS נחשב לבעל סמכות (Authoritative) על שם, אם הוא טוען את האזור המכיל שם זה. הרשומה הראשונה בכל קובץ אזור היא רשומת המשאב לתחילת הסמכות (SOA, **S**tart **o**f **A**uthority). רשומת משאב SOA מזהה שרת שמות DNS עיקרי עבור האזור כמקור המידע הטוב ביותר לנתונים באזור זה, וכיישות המעבדת את עדכוני האזור.

ניתן להאציל (Delegate) שמות בתוך האזור לאזורים אחרים. האצלה (Delegation) היא תהליך של שיוך האחריות על חלק ממרחב השמות של DNS ליישות נפרדת. יישות נפרדת זו יכולה להיות ארגון אחר, מחלקה, או קבוצת עבודה אחרת בתוך הארגון. במונחים טכניים, הכוונה בכך היא, שאתה מאפשר לאזור (או אזורים) אחר(ים) לנהל חלק ממרחב השמות של DNS שלך. רשומת שרת השמות המציינת אזור מואצל (Delegated Zone) ואת שם ה-DNS של השרת בעל הסמכות על אזור זה, מייצגת האצלת סמכות כגון זו. האצלת סמכויות בין אזורים מרובים היתה חלק מהמטרות המקוריות בתכנון DNS.

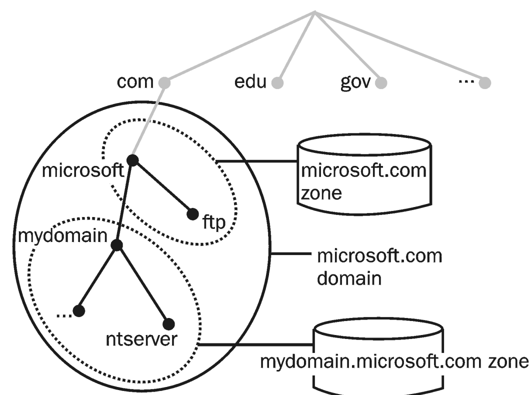
הרשימה הבאה מפרטת את הסיבות העיקריות להאצלת סמכות במרחב שמות DNS:

❖ הצורך להאציל סמכות ניהול של DNS domain למספר ארגונים או מחלקות בתוך הארגון.

❖ הצורך לבזר את טעינת מסד נתוני DNS גדול אחד בין מספר שרתי שמות, כדי לשפר את ביצועי הסדרת השמות, כמו גם ליצור סביבת DNS בעלת Fault Tolerance גבוהה.

❖ הצורך לאפשר צירוף של מארחים מהארגון, על ידי הכללתם ב-Domains המתאימים.

רשומת המשאבים של שרת השמות מקלה על האצלת הסמכות, בכך שהיא מזהה את שרתי ה-DNS עבור כל אזור. הם מופיעים בכל אזורי החיפוש לפנים או לאחור (Reverse/Forward Lookup Zones). בכל פעם ששרת DNS צריך לחצות את קווי הסמכות שלו, הוא יפנה לרשומת המשאבים של שרת השמות כדי לקבל את כתובתו של שרת ה-DNS באזור היעד. בתרשים 8.1, ניהולו של microsoft.com domain מחולק לשני אזורים, microsoft.com ו- mydomain.microsoft.com.



תרשים 8.1 ה-doamin בשם microsoft.com מאציל את סמכותו על שני אזורים נפרדים

הערה אם קיימות מספר רשומות שרתי שמות עבור אזור מואצל והן מזהות מספר שרתי DNS הזמינים לצורך שאילתה, יוכל שרת ה-DNS של Windows 2000 לבחור את שרת ה-DNS הקרוב אליו ביותר. הוא עושה זאת על ידי מדידת משך הזמן של תעבורה הלוך-ושוב (Round-Trip Intervals) הנמדדת מול כל שרת DNS.

הבנת אזורי DNS ו- Domains

שרתי שמות של domain מאחסנים מידע אודות חלק ממרחב השמות של ה-domain, הנקרא אזור (Zone). שרת שמות הוא הסמכות העליונה של אזור מסוים. שרת שמות יחיד יכול להיות בעל סמכות על אזורים רבים. תפיסת ההבדל שבין אזור ל-domain עשויה להיות מעט מבלבלת.

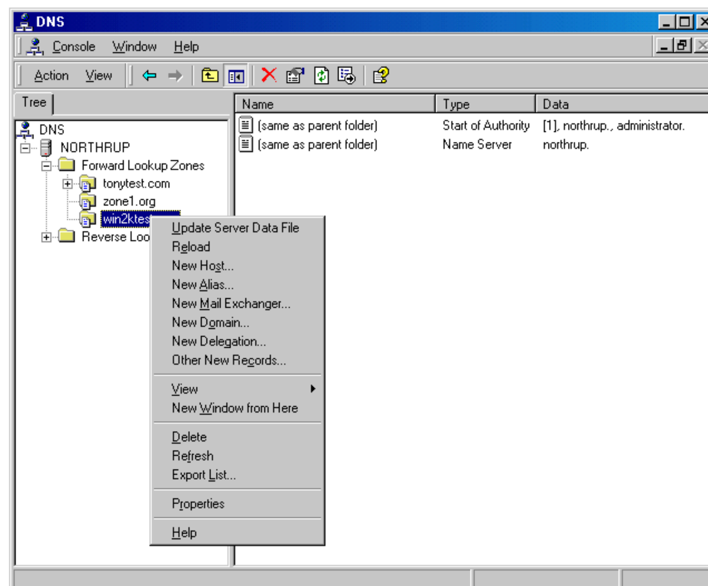
אזור הוא בפשטות חלק מ-domain. למשל, ה-domain בשם microsoft.com יכול להכיל את כל המידע אודות microsoft.com, marketing.microsoft.com ו- development.microsoft.com. אבל, האזור microsoft.com מכיל רק את המידע עבור microsoft.com ומפנה לשרתי השמות שהם בעלי הסמכות על Subdomains. האזור microsoft.com יכול להכיל את הנתונים עבור Subdomains של microsoft.com, אם לא הועברה הסמכות עליהם לשרת אחר. לדוגמה, marketing.microsoft.com יכול

לנהל את האזור המואצל של עצמו. האב, microsoft.com, יכול לנהל את development.microsoft.com. אם לא קיימים Subdomain, אזי ה-domain והאזור אחד הם. במקרה כגון זה, מכיל האזור את כל נתוני ה-domain.

הערה כל ה-Domains (ו- Subdomains) המופיעים כחלק מהאצלת האזור המדוברת חייבים להיוותר באזור הנוכחי קודם לביצוע האצלת הסמכות, כפי שמתוארת כאן. היעזר ב- MMC של DNS לפי הצורך, כדי קודם כל להוסיף Domains לאזור, לפני יישום הליך זה בפועל.

➤ כדי ליצור האצלת סמכות של אזור

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ולחץ DNS.
2. ב- MMC Tree, לחץ הציחה ימנית על ה-subdomain שלך, ומתפריט הקיצור בחר New Delegation, כפי שמוצג בתרשים 8.2.



תרשים 8.2 הוספת תרש האצלה נוסף

3. לחץ Next.
4. בתיבת דו-שיח Delegated Domain Name הקלד את שם ה-domain המואצל לסמכות, ולחץ Next.
5. בתיבת דו-שיח Name Servers לחץ Add וציין את השמות וכתובות ה-IP של שרתי ה-DNS שאתה מעוניין שיאחרו את האזורים המואצלים.

תופיע תיבת דו-שיח New Resource Record, בה תוכל לציין שרתי DNS.

6. הקלד את שם שרת ה-DNS, לחץ Add ולחץ OK.

7. בתיבת דו-שיח Name Servers לחץ Next.

8. לחץ Finish כדי לסגור את New Delegation Wizard.

הגדרת אזורים לעדכונים דינמיים

במקורו, נועד DNS לתמיכה רק בשינויים סטטיים למסד נתוני אזור. בשל מגבלות העיצוב החלות על DNS סטטי, ניתן היה להוסיף, להסיר או לשנות רשומות משאבים באופן ידני, על ידי מנהל מערכת DNS בלבד. למשל, מנהל מערכת DNS היה עורך רשומות בשרת העיקרי של האזור, ואז היה צריך להפיץ את מסד הנתונים המתוקן לשרתים המשניים בעת העברת אזור (Zone Transfer). אופן פעולה זה יכול לעשות את העבודה כשמספר השינויים קטן, והעדכונים מתבצעים לעיתים רחוקות יחסית, אבל במקרים אחרים הוא הופך לבלתי ניתן לניהול.

Windows 2000 מספקת תמיכה בלקוח ובשרת לשימוש בעדכונים דינמיים. עדכונים דינמיים מאפשרים למחשבי לקוח DNS לרשום ולעדכן באופן דינמי את רשומות המשאבים שלהם בשרת ה-DNS, בכל פעם שמתרחש שינוי. דבר זה מפחית את הצורך בניהול ידני למסד הנתונים של רשומות האזור, במיוחד עבור לקוחות אשר משנים מיקום לעיתים קרובות ומשתמשים בשרת DHCP להקצאת כתובת ה-IP שלהם.

כברירת מחדל, מחשבים בהם פועלת מערכת ההפעלה Windows 2000 ואשר הגדרות TCP/IP בהן מבוצעות באופן ידני, מנסים לרשום באופן דינמי רשומות משאבים של המארח ושל המצביע (Pointer) עבור כתובות IP המוגדרות והמשמשות את חיבורי הרשת המותקנים בהם. עדכונים דינמיים יכולים להישלח בשל כל אחת מהסיבות הבאות, או האירועים:

- ❖ כתובת IP הוספה, הוסרה או שונתה בהגדרות מאפייני TCP/IP של אחד או כל חיבורי הרשת המותקנים.
- ❖ חכירת (Lease) כתובת IP שונתה או חודשה בשרת ה-DHCP עבור אחד או כל חיבורי הרשת המותקנים; לדוגמה, כאשר המחשב מופעל או כאשר מבוצעת הפקודה ipconfig/renew.
- ❖ הפקודה ipconfig/registerdns מופעלת באופן ידני כדי לחייב רענון של רישום שם הלקוח ב-DNS.
- ❖ כאשר המחשב כבה.

דרישות לעדכון דינמי

עבור שרתי DNS, שירות ה-DNS יכול לאפשר או שלא לאפשר עדכונים דינמיים על בסיס אזור, בכל שרת המוגדר לטעון אזור עיקרי סטנדרטי או אזור משולב מדריך (Directory Integrated). כברירת מחדל, מחשבי לקוח הפועלים בסביבת אחת מבין מערכות ההפעלה ממשפחת Windows 2000 מעדכנים באופן דינמי את רשומות המשאבים של

המארח שלהם ב-DNS, כאשר מוגדר בהם TCP/IP. כאשר אזורי DNS מאוחסנים ב- Active Directory, DNS מוגדר כברירת מחדל לקבל עדכונים דינמיים.

הערה שרתי DNS של Windows 2000 **תומכים בעדכון דינמי. שרת ה-DNS המסופק עם מערכת ההפעלה** Windows NT **גירסה 4.0 אינו תומך בהם.**

כדי שתבוצע בקשה לעדכון דינמי, ניתן להגדיר מספר תנאי קדם. כל תנאי קדם חייב להתמלא במלואו כדי שהעדכון יבוצע. לאחר שכל התנאים התמלאו, יכול השרת העיקרי של האזור להמשיך ולעדכן את האזורים המקומיים שלו. הנה מספר דוגמאות לתנאי קדם שניתן להגדיר:

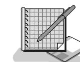
- רשומת משאב או ערכת רשומות משאבים כבר קיימות, או שהן בשימוש קודם לביצוע העדכון.
- רשומת משאב או ערכת רשומות משאבים אינן קיימות, או שהן אינן בשימוש קודם לביצוע העדכון.
- מבקש (Requester) יכול ליזום עדכון של רשומת משאב מסוימת או של ערכת רשומות משאבים.

כדי שמחשבי לקוח יירשמו ויעודכנו באופן דינמי בשרת DNS:

- התקן או שדרג מחשבי לקוח למערכת הפעלה Windows 2000,

  או

- התקן והשתמש בשרת DHCP של Windows 2000 ברשת שלך, כדי להחכיר למחשבי הלקוח ברשת שלך.

 תרגול: אפשור עדכונים דינמיים

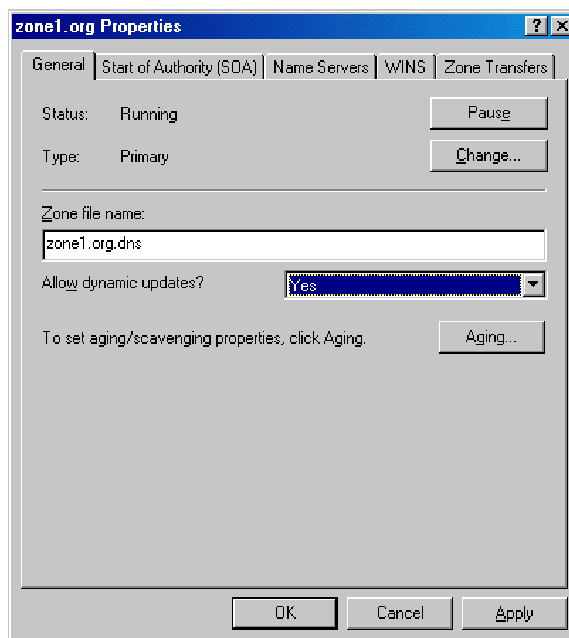
בתרגול זה תאפשר למחשבי לקוח DNS לרשום ולעדכן באופן דינמי את רשומות המשאבים שלהם בשרת DNS, בכל פעם שמתבצעים בהם שינויים. אתה עושה זאת על ידי אפשור עדכונים דינמיים באזור DNS.

➢ כדי לאפשר עדכונים דינמיים

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools ולחץ על DNS.

   מופיע MMC DNS.
2. ב- MMC Tree, לחץ לחיצה ימנית על האזור שלך ומתפריט הקיצור בחר Properties.

   מופיעה תיבת דו-שיח Zone Properties, כפי שנראה בתרשים 8.3.
3. מתיבת הרשימה הנפתחת ליד ?Allow dynamic updates בחר באפשרות Yes.
4. לחץ OK לסגירת תיבת דו-שיח Zone Properties.
5. סגור את DNS MMC.



תרשים 8.3 תיבת דו-שיח Zone Properties

סיכום שיעור

האצלת סמכות היא תהליך של הטלת אחריות על חלק ממרחב השמות ליישות נפרדת. רשומות המשאבים של שרת השמות מקלות על האצלת הסמכות על ידי זיהוי שרתי DNS עבור כל אזור. הן מופיעות בכל אזורי החיפוש לפנים ולאחור (Forward/Reverse Lookup Zones). Windows 2000 מספקת תמיכה בעדכונים דינמיים ללקוחות ולשרתים. עדכונים דינמיים מאפשרים למחשבי לקוח DNS לרשום ולעדכן באופן דינמי את רשומות המשאבים שלהם בשרת ה-DNS, בכל פעם שמתרחש שינוי.

שיעור 2: עבודה עם שרתים

מכיון שלשרתי DNS יש חשיבות תהומית ברוב סביבות המחשוב, חשוב לנטר אותם על בסיס קבוע. בשיעור זה תלמד כיצד לנהל ולנטר את שרתי ה-DNS שלך. בנוסף, תלמד כיצד ליישם שרת מיטמון-בלבד (Caching-Only Server).

לאחר שיעור זה, תוכל

- להגדיר שרת מיטמון-בלבד.
- לנהל ולנטר שרתי DNS.

זמן לימוד משוער: 15 דקות

סקירת שרתי DNS ומיטמון

שרתי DNS מעבדים שאילתות לקוח באמצעות רקורסיה או איטרציה. בדרך זו הם מגלים ומאחסנים כמות אדירה של מידע אודות מרחב השמות של DNS. השרת מטמין מידע זה. הטמנת המידע מאפשרת זירוז ביצועי הסדרת השמות של שרת DNS עבור שאילתות עוקבות אחר שמות פופולריים, בעוד שהיא מפחיתה במידה ניכרת את תעבורת הרשת הקשורה ב-DNS.

כששרתי DNS מבצעים שאילתה רקורסיבית בשמו של הלקוח, הם אוגרים באופן זמני במטמון רשומות משאבים. רשומות משאבים מוטמנות מכילות מידע שהושג משרתי DNS שהם בעלי סמכות על שמות DNS domains, שנלמדו תוך ביצוע שאילתות איטרטיביות לחיפוש, ועונים באופן מלא לשאילתה רקורסיבית שבוצעה בשמו של לקוח. בשלב מאוחר יותר, כאשר לקוחות אחרים מבצעים שאילתות חדשות הדורשות מידע רשומות משאבים התואם לרשומות משאבים השמורות במטמון, שרת ה-DNS יכול להשתמש במידע רשומות המשאבים המוטמן, כדי להשיב עליהן.

כאשר מידע מוטמן, נוסף לכל רשומות המשאבים המוטמנות ערך TTL (**T**ime-**T**o-**L**ive). כל עוד שמשך הזמן הקבוע בערך TTL אינו פג עבור רשומת משאבים מוטמנת, יכול שרת DNS להמשיך להטמין ולהשתמש ברשומת המשאבים שוב, כשהוא משיב לשאילתות המבוצעות על ידי הלקוחות שלו ואשר תואמות לרשומות משאבים אלו. ערכי TTL למידע המוטמן בעבור רשומות המשאבים ברוב תצורות האזורים מוגדר לערך מינימלי (ברירת המחדל), אשר מוגדר ברשומת משאב SOA של האזור. כברירת מחדל, TTL מינימלי מוגדר למשך של 3600 שניות (שעה אחת), אך ניתן לשנות זאת, אם יש צורך בכך, או שניתן לקבוע משכי TTL פרטניים לכל רשומת משאב.

יישום שרת מיטמון-בלבד

למרות שכל שרתי שמות DNS מטמינים שאילתות שהם מסדירים, שרתי מיטמון-בלבד (Caching-Only Servers) הם שרתי שמות DNS שרק מבצעים שאילתות, מטמינים את התשובות ומחזירים את התוצאות. אין להם סמכות על אף domains, והמידע האגור בהם מוגבל רק למה שהוטמן בעת הסדרת שאילתות. היתרון שמציג שרת מיטמון-בלבד טמון בכך שהם אינם יוצרים תעבורת רשת, מכיון שהם אינם מכילים אזורים כלשהם. אבל, יש

לדבר גם חיסרון אחד: כאשר השרת מופעל לראשונה אין בו כל מידע מוטמן ועליו לבנות מידע זה עם הזמן, כאשר מתבקשים שירותיו.

➤ כדי להתקין שרת DNS מיטמון-בלבד

1. התקן את שירות שרת DNS במחשב.

מומלץ מאוד, כאשר מפעילים מחשב כשרת DNS, לבצע את הגדרות TCP/IP באופן ידני ולקבוע למחשב זה כתובת IP קבוע.

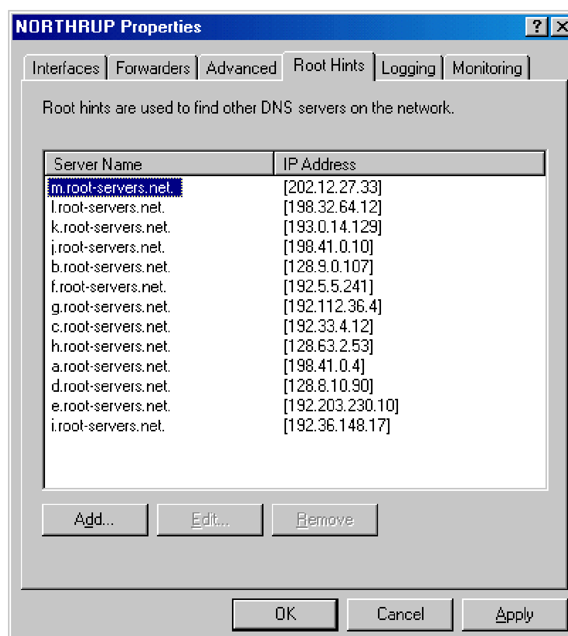
2. אל תגדיר את שרת ה-DNS לטעינת אזור כלשהו.

שרת DNS מיטמון-בלבד יכול להיות בעל ערך לאתר בו נדרשת פעילות DNS, אך אין זה רצוי מבחינה ניהולית ליצור domain או אזור נפרד עבור מיקום זה. שרתי DNS מיטמון-בלבד אינם מארחים Domains כלשהם ואינם בעלי סמכות ב-domain מסוים. אלה שרתי DNS הבונים מטמון שמות בשרת המקומי, אשר נלמד תוך כדי ביצוען של שאילתות רקורסיביות בשמם של לקוחותיו. לאחר מכן זמין מידע זה מהמטמון, כאשר מתבקשת תשובה לשאילתות עוקבות.

3. ודא שרמזים של שורש השרת מוגדרים או מעודכנים כהלכה.

כאשר מופעל שרת ה-DNS הוא זקוק לרשימת "רמזים" (Hints) של שרת השורש (Root Server). רמזים אלה הם רשומות NS (**N**ame **S**erver, שרת שמות) ו-A (Address, כתובת) של שרתי השורש, אשר בעבר נקראו קבצי המטמון (Cache Files).

אתה יכול להגדיר את רמזי השורש על ידי בחירה בכרטיסיה Root Hints שבתיבת דו-שיח Properties של שרת ה-DNS, ב- DNS MMC. כרטיסיה זו מוצגת בתרשים 8.4.


NORTHRUP Properties

Server Name	IP Address
m.root-servers.net.	[202.12.27.33]
l.root-servers.net.	[198.32.64.12]
k.root-servers.net.	[193.0.14.129]
j.root-servers.net.	[198.41.0.10]
b.root-servers.net.	[128.9.0.107]
f.root-servers.net.	[192.5.5.241]
g.root-servers.net.	[192.112.36.4]
c.root-servers.net.	[192.33.4.12]
h.root-servers.net.	[128.63.2.53]
a.root-servers.net.	[198.41.0.4]
d.root-servers.net.	[128.8.10.90]
e.root-servers.net.	[192.203.230.10]
i.root-servers.net.	[192.36.148.17]

תרשים 8.4 הכרטיסיה Root Hints שבתיבת דו-שיח Properties של שרת ה-DNS

ניטור ביצועי שרת DNS

מכיון ששרתי DNS הם בעלי חשיבות מכריעה ברוב סביבות העבודה הממוחשבות, ניטור ביצועיהם עשוי לספק בוחן ביצועים (Benchmark) יעיל לצפייה, הערכה ומיטוב ביצועיו של שרת DNS. בנוסף, תוכל לזהות במהרה ירידה בביצועי השרת במשך הזמן, או בעיתות עומס. Windows 2000 Server מספק ערכה של מוני ביצועים עבור DNS בהם ניתן להשתמש מתוך System Monitor כדי למדוד ולנטר היבטים שונים של פעילות השרת.

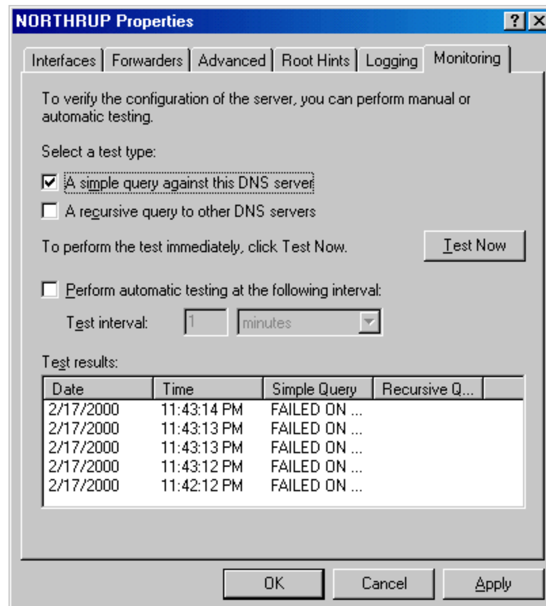
תרגול: בדיקת שאילתה פשוטה בשרת DNS

בתרגול זה תשתמש ב- DNS MMC כדי לבחון שאילתה פשוטה בשרת ה-DNS שלך.

➤ כדי לבחון שאילתה בשרת ה-DNS שלך

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ולחץ על DNS.
2. ב- MMC Tree לחץ לחיצה ימנית על שרת ה-DNS, ומתפריט הקיצור בחר Properties.
3. בחר בכרטיסיה Monitoring, הנראית בתרשים 8.5.
4. סמן את תיבת הסימון A simple query against this DNS server.
5. לחץ על Test Now.

   תוצאות השאילתה מוצגות בתיבה Test Results.
6. לחץ OK כדי לסגור את תיבת דו-שיח Properties של שרת ה-DNS.



תרשים 8.5 הכרטיסיה Monitoring בתיבת דו-שיח Properties של שרת ה-DNS

מוני ביצועים של שרת DNS

מערכת ההפעלה Windows 2000 Server כוללת ערכה של מוני ביצועים עבור שרת DNS, בהם ניתן להשתמש כדי למדוד ולנטר היבטים שונים של פעילות השרת, כגון:

- ❖ סטטיסטיקה של הביצועים הכוללים של השרת, כגון מספרן הכולל של שאילתות ותגובות שעובדו על ידי השרת.
- ❖ מוני UDP (**U**ser **D**atagram **P**rotocol) ו-TCP (**T**ransport **C**ontrol **P**rotocol), למדידת שאילתות ותגובות DNS שעובדו בכל אחד מפרוטוקולי התעבורה.
- ❖ מוני עדכון אוטומטי ועדכון אוטומטי מאובטח, למדידת פעילות רישום ועדכון הנוצרת על ידי לקוחות דינמיים.
- ❖ מוני שימוש בזיכרון, למדידת שימוש בזיכרון המערכת ותבניות הקצאת זיכרון הנוצרים על ידי הפעלת מחשב השרת כשרת DNS של Windows 2000.
- ❖ מוני חיפוש רקורסיבי למדידת שאילתות ותגובות, כאשר שירות שרת ה-DNS מבצע שאילתה רקורסיבית ומסדיר במלואם שמות DNS בשמם של הלקוחות המבקשים זאת.
- ❖ מוני חיפוש WINS למדידת שאילתות ותגובות שמבוצעות לשרת WINS, כאשר נעשה שימוש בתכונות חיפוש WINS המשולבות בשירות השרת של DNS.
- ❖ מוני העברת אזור, כולל מונים ייחודיים למדידת העברת אזור כללית (AXFR, All-Zone Transfer), העברת אזור מצטברת (Incremental Zone Transfer) והודעות עדכון אזור של DNS.

ניהול מרחוק של שרתי DNS

DNS הוא שירות שמות סטנדרטי של האינטרנט ושל TCP/IP, ומאפשר לשרת המפעיל את שירות DNS לאפשר למחשבי לקוח ברשת שלך להירשם ולהסדיר שמות DNS domains. שמות אלה יכולים לשמש לאיתור וגישה למשאבים המוצעים על ידי מחשבים אחרים באינטרנט. באמצעות Windows 2000 Administration Tools (כלי הניהול של Windows 2000), אותם ניתן למצוא בתקליטורי ההתקנה המקוריים של מערכות ההפעלה Windows 2000 Server ו- Windows 2000 Advanced Server, תוכל לנהל שרת מרחוק, מכל מחשב בו פועלת מערכת ההפעלה Windows 2000.

כלי הניהול של Windows 2000 מכילים יישום Snap-In עבור MMC (**M**icrosoft **M**anagement **C**onsole) וכלי ניהול נוספים המשמשים לניהול מחשבים הפועלים בסביבת Windows 2000 Server. כלים אלה אינם מסופקים בתקליטור ההתקנה של Windows 2000 Professional. לאחר שכלי הניהול מותקנים במחשב, יכול מנהל המערכת לפתוח את הכלי הנחוץ ולהתחיל לנהל שרת מרוחק ממחשב זה.

סיכום שיעור

למרות שרוב שרתי שמות DNS מטמינים את השאילתות אותן הסדירו, שרתי מיטמון-בלבד הם שרתי שמות DNS אשר רק מבצעים שאילתות, מטמינים את התשובות ומחזירים את התוצאות. יתרונם של שרתי מיטמון-בלבד טמון בכך שהם אינם גורמים לתעבורת רשת בהעברת אזור, מפני שהם אינם כוללים אזורים כלשהם. מערכת ההפעלה Windows 2000 Server מספקת ערכה של מוני ביצועים לשרתי DNS, אותם ניתן להפעיל באמצעות SYSTEM MONITOR כדי למדוד ולנטר את ההיבטים השונים של פעילות השרת. כדי לבצע בדיקות בשרת DNS תוכל להיעזר בכרטיסיה Monitoring שבתיבת דו-שיח Properties של שרת ה-DNS, מחלון DNS MMC. כדי לנהל מרחוק שרת, תוכל להיעזר ב- Windows 2000 Administration Tools. ניהול מרחוק יכול להתבצע מכל מחשב הפועל בסביבת Windows 2000.

שאלות סיכום

השאלות הבאות נועדו לחזק את הנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות על שאלה, עיין בשיעור המתאים ונסה את השאלה שנית. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואחר כך בעברית.

Answering the following questions will reinforce key information presented in this chapter. If you are unable to answer a question, review the appropriate lesson and then try the question again. Answers to the questions can be found in Appendix A, "Questions and Answers".

1. How many zones can a single DNS server host?
2. What benefits do DNS clients obtain from the dynamic update feature of Windows 2000?
3. Name one benefit and one disadvantage of a caching-only server.
4. List and describe three DNS performance counters.

1. כמה אזורים יכול לארח שרת DNS יחיד?
2. מהם יתרונות תכונת העדכון הדינמי של Windows 2000 ללקוחות DNS?
3. מנה יתרון אחד וחיסרון אחד לשרת מיטמון-בלבד?
4. מנה ותאר שלושה מוני ביצועים של DNS.

פרק 9

יישום WINS
Windows Internet Name)
(Service

אודות פרק זה

למרות ששרתי WINS (**W**indows **I**nternet **N**ame **S**ervice) אינם נדרשים ברשת המושתתת כולה על מחשבים מבוססי-Windows 2000, הם הכרחיים ברובן המכריע של רשתות TCP/IP המכילות מחשבים המבוססים על ארכיטקטורות ישנות יותר של Windows NT 4.0, Windows 98 או Windows 95. בפרק זה תלמד כיצד ליישם את WINS ברשת שלך.

לפני שתתחיל

להשלמת פרק זה צריך שיהיה ברשותך:

- ❖ מחשב בו מותקנת מערכת ההפעלה Windows 2000 Server, ובה מוגדר פרוטוקול TCP/IP.

שיעור 1: סקירת WINS

WINS מספק מסד נתונים מבוזר לרישום וביצוע שאילתות למיפוי דינמי של שמות NetBIOS, עבור מחשבים וקבוצות הפועלים ברשת שלך. WINS ממפה את שמות NetBIOS לכתובות IP, ותוכנן לפתור את הבעיות הנובעות מהסדרת שמות NetBIOS בסביבה מנותבת. WINS הוא הבחירה הטובה ביותר להסדרת שמות NetBIOS ברשתות מנותבות המשתמשות ב- NetBIOS over TCP/IP.

לאחר שיעור זה, תוכל

- לתאר את היחסים שבין NetBIOS ל- TCP/IP.
- לתאר את היתרונות שבשימוש ב-WINS.
- לתאר תכונה חדשה של Windows 2000 הקשורה ב-NetBIOS.

זמן לימוד משוער: 15 דקות

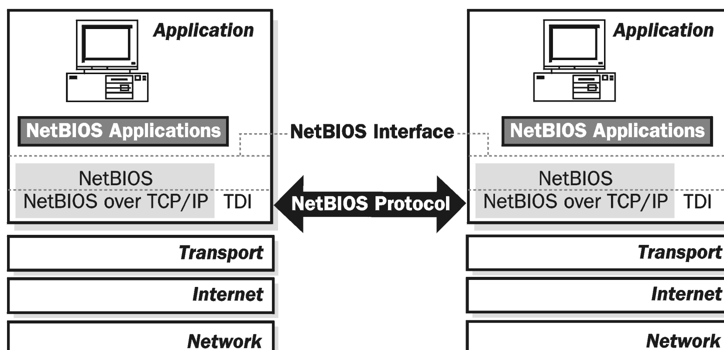
הסדרת שמות באמצעות NetBIOS

סעיף זה יסביר את התפיסה העומדת מאחורי הסדרת שמות NetBIOS ואת השיטות, כדי להקל עליך להבין טוב יותר את פעילותו של WINS. זאת, מכיון שגרסאות קודמות של מערכת ההפעלה Windows, כגון גירסה 4.0 של Windows NT ויישומים מבוססי-Windows מסוימים נעזרים בשמות NetBIOS, כדי לזהות משאבי רשת.

סקירת NetBIOS

NetBIOS תוכנן בשנת 1983 עבור חברת IBM על ידי חברה בשם Sytek Corporation, כדי לאפשר ליישומים לתקשר באמצעות רשת. כפי שמתואר בתרשים 9.1, NetBIOS מגדיר שתי יישויות:

- ❖ ממשק ברמת השיח (Session-Level Interface).
- ❖ פרוטוקול תעבורת ניהול/נתוני שיח (Session Management/Data Transport Protocol).



תרשים 9.1 תקשורת NetBIOS על TCP/IP

ממשק NetBIOS הוא ממשק תכנות יישומים (API, **A**pplication **P**rogramming **I**nterface) ברמת שכבת היישום (Application Layer) שנועד לשימושם של יישומים להגשת קלט/פלט רשת (Network I/O) ולשליטה בהפניות לפרוטוקולי הרשת הבסיסיים. תוכנית יישום המשתמשת בממשק API של NetBIOS לצורך תקשורת רשת יכולה לפעול בכל פרוטוקול התומך בממשק NetBIOS. הדבר מיושם על ידי תוכנת שכבת השיח (Session Layer), כגון NBFP (**N**et**B**IOS **F**rame **P**rotocol) או NetBT (NetBIOS over TCP/IP), כדי לבצע את קלט/פלט הרשת הנדרש לאחסון ערכת הפקודות של ממשק NetBIOS.

NetBIOS מספק פקודות ותמיכה לשירותים הבאים:

- ❖ וידוא ורישום שם רשת.
- ❖ הקמה וניתוק שיח.
- ❖ תעבורת נתוני שיח אמינה מוכוונת-חיבור.
- ❖ תעבורת נתוני צרורות נתונים בלתי אמינה חסרת חיבור.
- ❖ ניטור וניהול פרוטוקול תמיכה (מנהל התקן) והמתאם.

שמות NetBIOS

שם NetBIOS הוא כתובת ייחודית בת 16 סיביות המשמשת לזיהוי משאב NetBIOS ברשת. שם זה יכול להיות שם ייחודי (Unique, בלעדי) או קבוצה (Group, לא בלעדי). שמות ייחודיים משמשים בדרך כלל לשליחת תקשורת רשת להליך (Process) מסוים במחשב. שמות קבוצות משמשים לשליחת מידע למספר מחשבים בו-זמנית. דוגמה להליך המשתמש בשם NetBIOS הוא השירות File and Print service for Microsoft Network במחשב מבוסס Windows 2000. כאשר המחשב מאותחל רושם שירות זה שם NetBIOS ייחודי המבוסס על שם המחשב שלך. השם המדויק בו משתמש השירות הוא 15 תווי שם המחשב בנוסף לתו ה-16 מתוך 0x20. אם שם המחשב אינו באורך 15 תווים הוא מרופד (padded) ברווחים, עד שיכיל 15 תווים.

הסדרת שמות NetBIOS הוא תהליך של מיפוי שם NetBIOS של מחשב לכתובת IP. שם NetBIOS של מחשב חייב תמיד להיות מוסדר לכתובת IP לפני שניתן יהיה להסדיר את כתובת ה-IP לכתובת חומרה. TCP/IP של Microsoft משתמש במספר שיטות להסדרת שמות NetBIOS; אבל, המנגנון העיקרי המשמש להסדרת שמות NetBIOS לכתובות IP תלוי בסוג הצומת של NetBIOS אשר מוגדר לצומת. RFC 1001, אשר כותרתו היא Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Concepts and Methods, מגדיר את סוגי הצמתים של NetBIOS, כפי שניתן ללמוד מטבלה 9.1.

טבלה 9.1 סוגי צמתי NetBIOS

סוג הצמת	תיאור
B-Node (Broadcast)	B-Node משתמש בשאילתות שמות NetBIOS ב- Broadcast (Broadcast) לרישום והסדרת שם. ל- B-Node יש שתי בעיות עיקריות: (1) שידורים רחבים מטרידים כל צומת ברשת. (2) בדרך כלל נתבים אינם מעבירים שידורים רחבים, כך שניתן להסדיר רק שמות NetBIOS ברשת המקומית.
P-Node (Peer-Peer)	P-Node משתמש בשרת שמות NetBIOS, כגון שרת WINS, להסדרת שמות NetBIOS. P-Node אינו עושה שימוש ב- Broadcast; במקום זאת הוא מבצע שאילתות ישירות לשרת השמות.
M-Node (Mixed)	M-Node הוא שילוב של B-Node עם P-Node. כברירת מחדל, מתפקד M-Node כאילו היה B-Node. אם M-Node אינו מצליח להסדיר שם על ידי Broadcast, הוא מתשאל את שרת שמות NetBIOS באמצעות P-Node.
H-Node (Hybrid)	H-Node הוא שילוב של P-Node עם B-Node. כברירת מחדל, מתפקד M-Node כאילו היה P-Node. אם M-Node אינו מצליח להסדיר שם באמצעות שרת שמות NetBIOS, הוא ישתמש ב- Broadcast כדי לעשות כן.

מחשבי Windows 2000 הם צמתי B-Node כברירת מחדל, והופכים לצמתי H-Node כאשר מוגדר בהם שרת WINS. Windows 2000 יכולים גם להשתמש בקובץ מסד נתונים מקומי הנקרא LMHOSTS כדי להסדיר שמות NetBIOS מרוחקים. הקובץ LMHOSTS מאוחסן בתיקיה %SystemRoot%\System32\Drivers\Etc. קובץ LMHOSTS לדוגמה (LMHOSTS.SAM) נכלל גם הוא בתיקיה זו.

הקובץ LMHOSTS

הקובץ LMHOSTS הוא קובץ ASCII סטטי המשמש להסדרת שמות NetBIOS לכתובות IP של מחשבים מרוחקים הפועלים בסביבת Windows NT, או מארחים מבוססי-NetBIOS אחרים. תרשים 9.2 מציג לדוגמה קובץ LMHOSTS.

```
lmhosts - Notepad
File  Edit  Format  Help
# 102.54.94.97     rhino          #PRE #DOM:networking  #net group's DC
# 102.54.94.102    "appname  \0x14"                     #special app server
# 102.54.94.123    popular             #PRE             #source server
# 102.54.94.117    localsrv            #PRE             #needed for the incluc
#
# #BEGIN_ALTERNATE
# #INCLUDE \\localsrv\public\lmhosts
# #INCLUDE \\rhino\public\lmhosts
# #END_ALTERNATE
#
# In the above example, the "appname" server contains a special
# character in its name, the "popular" and "localsrv" server names are
# preloaded, and the "rhino" server name is specified so it can be used
# to later #INCLUDE a centrally maintained lmhosts file if the "localsrv"
# system is unavailable.
#
# Note that the whole file is parsed including comments on each lookup,
# so keeping the number of comments to a minimum will improve performance.
# Therefore it is not advisable to simply add lmhosts file entries onto the
# end of this file.
10.107.9.10             Mexico                    # Sales Server
10.107.7.29             France                    # Database Server
10.131.54.73            UK                        # Training Server
10.129.10.4             Sweden          #PRE      # Main Office Server
10.102.93.122           Austrailia      #PRE      # MIS Server
```

תרשים 9.2
קובץ
LMHOSTS

מילות מפתח מוגדרות מראש

קובץ LMHOSTS כולל גם מילות מפתח המוגדרות מראש המתחילות בסימן סולמית (#). אם אתה משתמש בקובץ LMHOSTS זה במערכת NetBT מיושנת, כגון LAN Manager, הפניות אלו אינן מבוצעות ומתייחסים אליהן כאל הערות, מפני שהן מתחילות בסימן מספר (Number Sign, #). טבלה 9.2 מציגה את מילות המפתח האפשריות בקובץ LMHOSTS:

טבלה 9.2 מילות מפתח של LMHOSTS

מילת מפתח מוגדרת	תיאור
#PRE	מגדיר איזה רשומות צריכות להיטען מראש כרשומות קבועות במטמון השמות. רשומות טעונות מראש מפחיתות את השידורים הרחבים ברשת, מפני שהשמות מוסדרים מהמטמון, ולא על ידי Broadcast או על ידי ניתוח הקובץ LMHOSTS. רשומות להן התגית #PRE נטענות באופן אוטומטי בעת אתחול, או באופן ידני על ידי הקלדת הפקודה nbstat - R במנחה שורת הפקודה.
#DOM:[domain_name]	מקל על פעילות ה- Domain, כגון פעולות אימות כניסה למערכת (Log On Validation) דרך נתב, סינכרון חשבונות ועיון (Browsing).
#NOFNR	מונע את השימוש בשאילתות המכוונות לשמות NetBIOS עבור מערכות UNIX LAN Manager ישנות.
#BEGIN_ALTERNATE #END_ALTERNATE	מגדיר רשימה יתירה של מיקומים חלופיים של קבצי LMHOSTS. הדרך המומלצת לכלול (#INCLUDE) קבצים מרוחקים היא על ידי שימוש בנתיב UNC (**U**niversal **N**aming **C**onvention), כדי להבטיח את הגישה לקובץ. מובן ששמות UNC חייבים להופיע בקובץ LMHOSTS כאשר שמות NetBIOS מתורגמים כהלכה לכתובות IP.
#INCLUDE	טוען ומחפש רשומות NetBIOS בקובץ נפרד מהקובץ LMHOSTS. בדרך כלל, קובץ #INCLUDE הוא קובץ LMHOSTS משותף המנוהל באופן מרוכז.
#MH	מוסיף מספר מרובה של רשומות, עבור מחשב בו מותקנים יותר מכרטיס רשת אחד (Multihomed).

סקירת WINS

WINS מבטל את הצורך בשידורים רחבים (Broadcast) להסדרת שמות מחשבים לכתובות IP, ומספק מסד נתונים דינמי השומר מיפוי של שמות מחשבים לכתובות IP. WINS הוא שרת שמות NetBIOS מורחב (NBNS, **N**et**B**IOS **N**ame **S**erver), שנועד על ידי Microsoft

למנוע תעבורת שידורים רחבים המשויכת ליישום צמתי B-Node של NetBT. הוא משמש לרישום שמות NetBIOS של מחשבים ולהסדיר אותם לכתובות IP, הן למחשב המקומי והן למארחים מרוחקים.

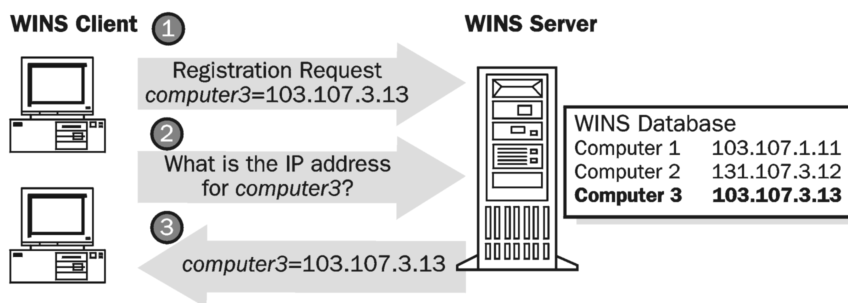
לשימוש ב-WINS קיימים מספר יתרונות. היתרון העיקרי טמון בכך שבקשות הלקוח להסדרת שם מחשב נשלחות ישירות לשרת WINS. אם שרת ה-WINS מסוגל להסדיר את השם הוא שולח את כתובת ה-IP ישירות ללקוח. כתוצאה מכך, לא נדרש Broadcast ופוחתת תעבורת הרשת. אבל, אם שרת WINS אינו זמין, עדיין יכול לקוח WINS להשתמש ב- Broadcast בניסיון להסדיר את השם. יתרון אחר בשימוש ב-WINS הוא שמסד הנתונים של WINS מעודכן באופן דינמי, כך שהוא תמיד עדכני. עובדה זו מפחיתה את הצורך בקובץ LMHOSTS. יתר על כן, WINS מספק אפשרויות עיון (Browsing) בין-תחומי (Interdomain) וברשת.

לפני ששני מארחים מבוססי-NetBIOS יוכלו לתקשר, חייב שם NetBIOS של היעד להיות מוסדר לכתובת IP. הדבר נחוץ מכיון ש-TCP/IP דורש כתובת IP, ולא שם NetBIOS של מחשב, כדי לתקשר. כפי שמודגם בתרשים 9.3, הסדרה מתבצעת על פי התהליך הבא:

בסביבת WINS, בכל פעם שמאותחל לקוח WINS הוא רושם את מיפוי שם NetBIOS/כתובת IP שלו בשרת WINS המוגדר בו.

כאשר לקוח WINS יוזם פקודה להתקשרות עם מארח אחר, נשלחת שאילתת השם ישירות לשרת ה-WINS, במקום שתשודר בכל רחבי הרשת המקומית.

אם שרת ה-WINS מאתר מיפוי שם NetBIOS/כתובת IP עבור מארח היעד במסד הנתונים שלו, הוא מחזיר ללקוח WINS את כתובת ה-IP של מארח היעד. מכיון שמסד הנתונים של WINS משיג את מיפוי שם NetBIOS/כתובת IP באופן דינמי, הוא תמיד עדכני.



תרשים 9.3 הסדרת שמות באמצעות WINS

WINS ו-Windows 2000

קודם ל-Windows 2000, כל מערכות ההפעלה MS-DOS ואלו המבוססות-Windows, צריכות היו את ממשק השמות של NetBIOS כדי לתמוך באפשרויות הרשת. עם יציאתה של Windows 2000 לאוויר העולם, התמיכה בממשק שמות NetBIOS כבר אינה נחוצה למחשבים המתקשרים ברשת, מפני שניתן שלא לאפשר NetBT עבור כל חיבור רשת. תכונה

זו נועדה עבור מחשבים הנעזרים רק בטכניקות רישום והסדרת שמות של DNS, ומתקשר עם מחשבים אחרים באמצעות הרכיבים Client for Microsoft Network ו-File and Print Service for Microsoft Network בהם NetBT אינו פעיל. דוגמאות למחשבים בהם NetBT אינו פעיל כוללות מחשבים שתפקידיהם מיוחדים או חסויים מהרשת, כגון שרת Proxy חיצוני (Edge Proxy Server) או מארח המבוצר מאחורי חומת אש (Firewall), כאשר תמיכה ב-NetBT אינה נדרשת או רצויה.

דוגמה נוספת היא סביבה המכילה מארחים ותוכניות התומכים בשימוש ב-DNS, אשר ניתן לבנות כך שיפעילו Windows 2000 ומערכות הפעלה אחרות שאינן דורשות שמות NetBIOS, כגון חלק מגרסאות UNIX. אבל, רוב הרשתות עדיין זקוקות לשלב מערכות הפעלה מיושנות הדורשות שמות רשת NetBIOS למחשבים הפועלים בסביבת Windows 2000. מסיבה זו, המשיכה Microsoft לספק תמיכת ברירת מחדל בשמות NetBIOS גם עם Windows 2000, כדי להקל על פעילות משולבת עם מערכות הפעלה מיושנות הדורשות זאת. תמיכה זו מסופקת בעיקרה בשני אופנים:

- ❖ כברירת מחדל, כל המחשבים בהם פועלת מערכת ההפעלה Windows 2000 המשתמשים ב-TCP/IP, מאפשרים תמיכת צד-לקוח לרישום והסדרת שמות NetBIOS.

  תמיכה זו מסופקת באמצעות NetBT וניתן, אם יש צורך בכך, לבטל אותה באופן ידני.

- ❖ Windows 2000 Server ממשיכה לספק תמיכת צד-שרת באמצעות WINS. WINS יכול לשמש לניהול יעיל של רשתות NetBT.

סיכום שיעור

יישומים אחדים וגרסאות קודמות של Windows משתמשים בשמות NetBIOS כדי לזהות משאבי רשת. WINS הוא NBNS מורחב שנועד על ידי Microsoft למנוע תעבורת שידורים רחבים המשויכים ליישום B-Node של NetBT. לשימוש ב-WINS קיימים מספר יתרונות, העיקרי שבהם הוא שתעבורת השידור מופחתת מפני שבקשות להסדרת שמות נשלחות ישירות לשרת WINS.

שיעור 2:
תהליך הסדרת השמות של WINS

לרישום, חידוש ושחרור שמות משתמש WINS בשיטות סטנדרטיות. שיעור זה מציג את השלבים השונים המשמשים בתהליך הסדרת שם NetBIOS לכתובת IP, תוך שימוש ב-WINS.

לאחר שיעור זה, תוכל

- לתאר תהליכי רישום, חידוש, שחרור, שאילתה ותגובה של WINS.

זמן לימוד משוער: 25 דקות

הסדרת שמות NetBIOS באמצעות WINS

כאשר לקוח צריך לתקשר עם מארח אחר ברשת, ראשית הוא מתקשר עם שרת ה-WINS, כדי להסדיר את כתובת ה-IP על ידי שימוש בנתוני המיפוי ממסד הנתונים של השרת. מנוע מסד הנתונים היחסי (Relational Database) של שרת WINS מבצע גישה למסד נתונים ISAM (Indexed Sequential Access Method). מסד הנתונים ISAM הוא שכפול של מסד הנתונים המכיל את המיפויים עבור שמות NetBIOS של המחשבים לכתובות ה-IP. כדי שלקוח WINS יוכל להיכנס לרשת הוא חייב לרשום את שם המחשב שלו ואת כתובת ה-IP בשרת WINS. דבר זה יוצר במסד נתוני WINS רשומה עבור כל שירות NetBIOS הפועל בלקוח. מכיון שרשומות אלו מעודכנות בכל פעם שלקוח מאופשר-WINS מתחבר לרשת, המידע המאוחסן במסד הנתונים של שרת WINS מועדכן תמיד.

ההליך בו משתמש WINS להסדר ושימור של שמות NetBIOS דומה ליישום של B-Node. השיטה המשמשת לחידוש שם היא ייחודית לצמתים מסוג NetBIOS, העושים שימוש בשרתי שמות NetBIOS. WINS הוא הרחבה של RFC 1001 ו- RFC 1002. תרשים 9.4 מציג את תהליך הסדרת שם NetBIOS.

רישום שם

לכל לקוח WINS מוגדרת כתובת שרת WINS עיקרי (Primary WINS Server), ואם קיים כזה, גם שרת WINS משני (Secondary WINS Server). כאשר מופעל הלקוח הוא רושם את שם NetBIOS שלו ואת כתובת ה-IP בשרת WINS המוגדר בו. שרת WINS מאחסן את מיפוי שם NetBIOS/כתובת IP במסד הנתונים שלו.

חידוש שם

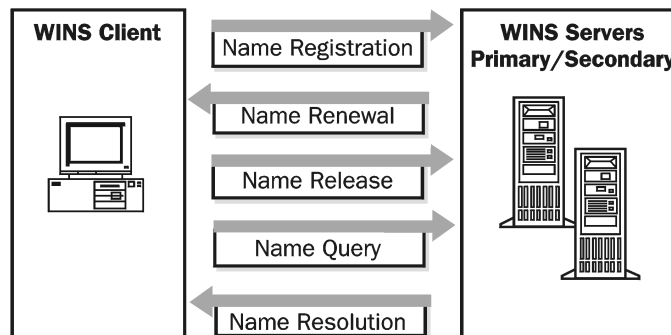
כל שמות NetBIOS נרשמים על בסיס זמני, מה שאומר שאותו שם יכול לשמש בשלב מאוחר יותר מארח שונה, אם המשתמש המקורי מפסיק להשתמש בו.

שחרור שם

כל לקוח WINS אחראי על שימור חוזה החכירה של שמו הרשום. כאשר לא נעשה יותר שימוש בשם, למשל במקרה שהמחשב מכובה, שולח לקוח WINS הודעה לשרת ה-WINS לשחרר אותו.

שאילתת שם והסדרת שם

לאחר שלקוח WINS רשם את שם NetBIOS שלו ואת כתובת ה-IP שלו אצל שרת ה-WINS, הוא יכול לתקשר עם מארחים אחרים על ידי השגת כתובת ה-IP של מחשבים מבוססי-NetBIOS אחרים, משרת WINS. כל התקשרויות WINS מתבצעות תוך שימוש בצרורות נתונים המכוונות דרך יציאה (Port) 137 של UDP (NBNS).



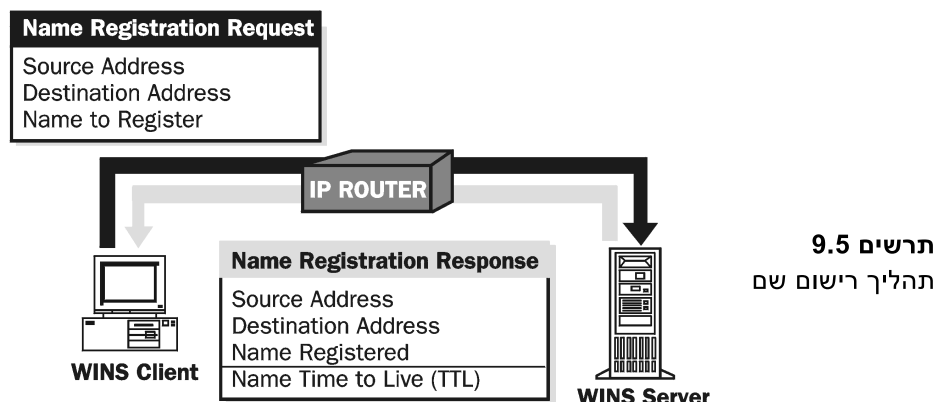
תרשים 9.4 הסדרת שמות בין לקוחות ושרת WINS

רישום שם

שלא כמו יישום B-Node של NetBT, אשר מבצע Broadcast של רישום שמו, לקוחות WINS רושמים את שם NetBIOS שלהם בשרתי WINS.

כאשר לקוח WINS מאותחל הוא רושם את שם NetBIOS שלו על ידי שליחת בקשה לרישום שם ישירות לשרת WINS המוגדר בו. שמות NetBIOS נרשמים כאשר יישומים או שירותים מאותחלים, כגון Workstation, Server או Messanger.

אם שרת WINS זמין והשם עדיין אינו רשום על ידי לקוח WINS אחר, מוחזרת ללקוח הודעה בדבר רישום מוצלח. הודעה זו מכילה את משך הזמן ששם NetBIOS זה רשום על שם הלקוח, שמצוין כ-TTL (**T**ime **T**o **L**ive). תרשים 9.5 מציג את תהליך רישום השם.



תרשים 9.5
תהליך רישום שם

כאשר נמצאת כפילות שמות

אם נרשמה במסד הנתונים של WINS כפילות של שמות, שולח שרת ה-WINS הזמנה לזיהוי (Challenge) לבעלים הנוכחי של השם. ההזמנה לזיהוי נשלחת כבקשה לשאילתת שם. שרת ה-WINS שולח את ההזמנה שלוש פעמים, במרווחי זמן של 500 אלפיות השנייה בין שליחה אחת לשנייה.

אם במחשב הרשום מותקן יותר מכרטיס רשת אחד (Multihomed), מנסה שרת ה-WINS כל כתובת IP עד שהוא מקבל תגובה, או עד אשר נוסו כל כתובות ה-IP.

אם הבעלים הרשום (Registered Owner) הנוכחי מגיב בהצלחה לשרת ה-WINS, שולח השרת תגובה שלילית ללקוח WINS המנסה לרשום שם זה. אם בעליו הרשום הנוכחי של השם אינו מגיב לשרת ה-WINS, שולח השרת תגובה לגבי רישום מוצלח של השם לאותו לקוח WINS המנסה לרשום שם זה.

כאשר שרת WINS אינו זמין

לקוח WINS יבצע שלושה ניסיונות לתקשר עם שרת WINS העיקרי המוגדר בו. אם אחרי הניסיון השלישי הוא נכשל בכך, תישלח הבקשה לרישום השם לשרת WINS המשני, אם כזה מוגדר לו. אם אף אחד משרתי ה-WINS אינו זמין, ייזום הלקוח Broadcast כדי לרשום את שמו.

חידוש שם

כדי להמשיך ולהשתמש באותו שם NetBIOS, חייב הלקוח לחדש את חוזה החכירה שלו (Lease) לפני שתוקפו פג. אם הלקוח אינו מחדש את חוזה החכירה, שרת WINS הופך את השם לזמין עבור לקוחות WINS אחרים.

בקשה לרענון שם

לקוחות WINS חייבים לחדש את רישום שמם, לפני שתוקפו של זה פג. מרווח החידוש (Renewal Interval) קובע את משך הזמן בו יאחסן השרת את רישום השם כרשומה פעילה במסד הנתונים של WINS. כאשר לקוח WINS מחדש את רישום שמו הוא שולח בקשה לרענון שם (Name Refresh Request) לשרת WINS. בקשה זו כוללת את כתובת ה-IP ואת שם NetBIOS אותו מבקש הלקוח לרענן. שרת ה-WINS מגיב לבקשה לרענון השם בתגובת רענון שם (Name Refresh Response), הכוללת את מרווח החידוש החדש לשם זה. כאשר לקוח מרענן את שמו הוא מבצע את הצעדים הבאים:

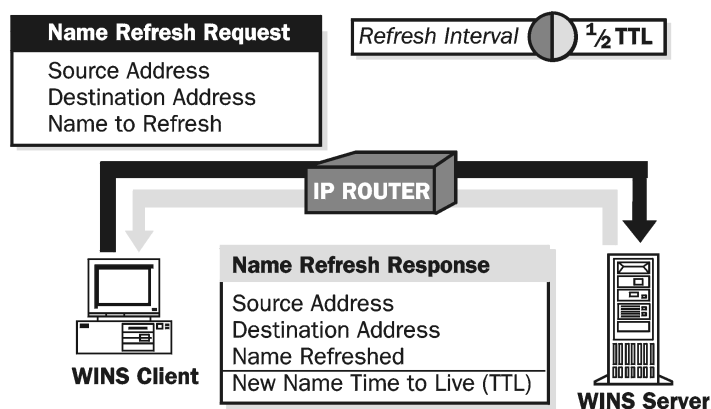
1. כאשר עבר חצי ממרווח החידוש (Renewal Interval) של הלקוח הוא שולח בקשה לחידוש השם לשרת WINS העיקרי.
2. אם השם אינו מחודש על ידי שרת ה-WINS העיקרי, מנסה הלקוח לרענן את השם מחדש אחרי 10 דקות, וממשיך לנסות לבצע חידוש בשרת WINS העיקרי כל 10 דקות, עד חלוף שעה אחת. אחרי שניסה לחדש את רישום שמו אצל שרת ה-WINS העיקרי למשך שעה, מפסיק לקוח WINS ומנסה לבצע את החידוש אצל שרת WINS המשני המוגדר לו.

3. אם גם שרת ה-WINS המשני אינו מרענן את רישום השם, מנסה לקוח ה-WINS לחדש את הרישום כל 10 דקות, עד חלוף שעה. אחרי שניסה לחדש את רישום שמו אצל שרת ה-WINS המשני למשך שעה, מפסיק לקוח WINS ושב לנסות את מזלו אצל שרת WINS העיקרי. תהליך זה של ניסיון אצל השרת העיקרי ואחר כך אצל המשני חוזר על עצמו עד שפג תוקף רישום השם, או עד ששם הלקוח מרוענן ומחודש.

4. אם לקוח ה-WINS מצליח לחדש את רישום שמו, מאופס מרווח החידוש בשרת ה-WINS.

5. אם הלקוח נכשל ברישום לכל אורך מרווח החידוש באחד מבין שני שרתי ה-WINS, העיקרי או המשני, השם משוחרר.

תרשים 9.6 מציג כיצד מחדש לקוח WINS את חוזה החכירה שלו לשימוש באותו שם NetBIOS.



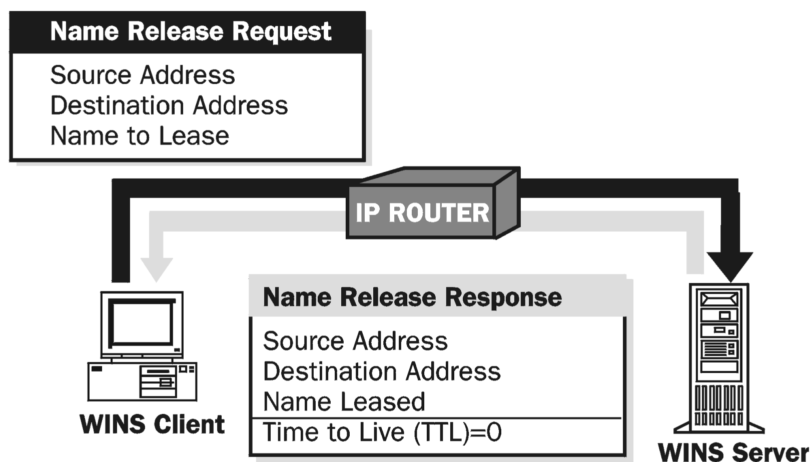
תרשים 9.6 חידוש חוזה חכירה לשימוש באותו שם NetBIOS

כאשר שרת WINS מקבל את הבקשה לחידוש השם הוא שולח ללקוח תגובה לחידוש השם, הכוללת ערך TTL חדש.

שחרור שם

כאשר לקוח WINS מכובה כהלכה, הוא שולח ישירות לשרת ה-WINS בקשה לשחרור השם עבור כל שם רשום שלו. הבקשה לשחרור השם (Name Release Request) כוללת את כתובת ה-IP של הלקוח ואת שם NetBIOS אותו יש להסיר ממסד הנתונים של WINS. דבר זה מאפשר לשם NetBIOS זה להיות פנוי לשימושו של לקוח אחר, כפי שמתואר בתרשים 9.7.

כאשר שרת WINS מקבל את הבקשה לשחרור שם, הוא בוחן את מסד הנתונים שלו כדי לאתר את השם המצוין בו. אם הוא נתקל בשגיאה, או במידה והמיפוי מצביע על כתובת IP שונה, נשלחת ללקוח תגובה שלילית (Negative Name Release) לגבי שחרור השם. אחרת, שולח שרת ה-WINS תגובה חיובית לשחרור השם ומסמן במסד הנתונים שלו שהשם המצוין אינו פעיל. תגובת שחרור השם כוללת את שם NetBIOS המשוחרר וערך 0 (אפס) של TTL.



תרשים 9.7 בקשה לשחרור שם

שאילתת שם ותגובת שם

שיטה שכיחה להסדרת שמות NetBIOS לכתובות IP היא באמצעות NBNS, כגון WINS. כברירת מחדל, כאשר מגדירים לקוח WINS, נעשה שימוש בסוג הצומת H-Node של NetBT. לפני ביצוע Broadcast, תמיד נבדק NBNS לאיתור מיפויי כתובות IP/שמות NetBIOS. הצעדים הבאים, אשר מתוארים גם בתרשים 9.8, מתארים את התהליך:

כאשר המשתמש יוזם פקודת Windows NT, כגון net use, נבדק מטמון שמות NetBIOS כדי לאתר בו את מיפוי שם NetBIOS/כתובת IP של המארח האחר.

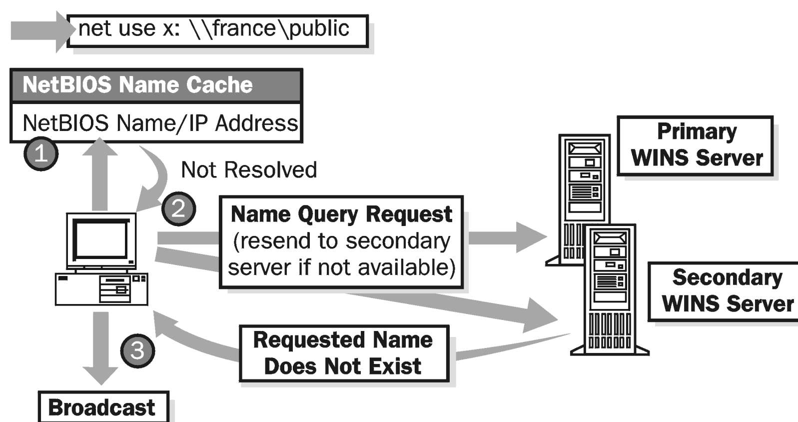
אם השם אינו מוסדר מהמטמון, נשלחת בקשה לשאילתת שם ישירות לשרת WINS העיקרי של הלקוח.

אם שרת WINS העיקרי של הלקוח אינו זמין, שב הלקוח ושולח את הבקשה ישירות פעמיים נוספות, לפני שיפנה לשרת WINS המשני.

כאשר אחד מהשרתים מסדיר את השם נשלחת ללקוח המקור תגובה חיובית, הכוללת את כתובת ה-IP המשויכת לשם NetBIOS המבוקש.

במידה ואף אחד מהשרתים אינו מצליח להסדיר את השם, נשלחת ללקוח WINS תגובה לשאילתת שם ובה ההודעה Requested name does not exist (השם המבוקש אינו קיים), ואז מתבצע Broadcast.

אם השם אינו מוסדר מהמטמון על ידי שרת ה-WINS או באמצעות Broadcast, ייתכן שניתן יהיה עדיין להסדיר אותו על ידי ניתוח קובץ LMHOSTS או HOSTS, או על ידי שימוש ב-DNS.



תרשים 9.8 שרת שמות NetBIOS מנסה לאתר מיפוי שם NetBIOS/כתובת IP

סיכום שיעור

WINS משתמש בשיטות סטנדרטיות לרישום, חידוש ושחרור שמות. כדי להמשיך ולהשתמש באותו שם NetBIOS, חייב הלקוח לחדש את חוזה החכירה של השם לפני שיפוג תוקפו. כאשר לקוח WINS מכובה כהלכה הוא מודיע לשרת ה-WINS שאינו זקוק יותר לשם NetBIOS.

שיעור 3: יישום WINS

ברשתות בהן השרתים פועלים בסביבת Windows 2000 Server וכל תחנות העבודה פועלות בסביבת Windows 2000 Professional, NetBIOS כבר אינו נדרש לשם תקשורת מבוססת TCP/IP. בשל שינוי זה WINS נחוץ ברוב הרשתות, אך ייתכן שבמקרים מסוימים לא יהיה צורך בו. בשיעור זה תלמד כיצד ליישם את WINS ברשת שלך.

לאחר שיעור זה, תוכל

- להתקין ולהגדיר שרת WINS.
- להתקין ולהגדיר לקוח WINS.
- לאתר ולטפל בתקלות בשרתים ובלקוחות WINS.
- לנהל ולנטר WINS.

זמן לימוד משוער: 40 דקות

מתי להשתמש ב-WINS

כאשר עליך להחליט אם אתה צריך או לא להשתמש בשרת WINS, שאל את עצמך את השאלות הבאות, בתור שלב ראשון:

- **האם יש לי ברשת מחשבים מיושנים או יישומים הדורשים שימוש בשמות NetBIOS?** זכור שכל המחשבים המרושתים בהם פועלות מערכות הפעלה קודמות של Microsoft, כגון גרסאות DOS, Windows או Windows NT, דורשות תמיכה בשמות NetBIOS. Windows 2000 היא מערכת ההפעלה הראשונה מבית Microsoft שאינה דורשת מיעון NetBIOS. בשל כך, ייתכן ששמות NetBIOS עדיין יהיו דרושים ברשת שלך, כדי לספק תמיכה בשירותי קבצים והדפסה בסיסיים עבור יישומים מיושנים (Legacy Applications) רבים בהם עדיין נעשה שימוש.
- **האם כל המחשבים ברשת שלי מוגדרים ומאפשרים תמיכה בסוג אחר של מיעון שמות רשת, כגון DNS?** מיעון שמות הוא עדיין שירות חיוני לאיתור מחשבים ומשאבים ברשת שלך, גם כאשר שמות NetBIOS אינם נחוצים. לפני שתחליט לבטל את התמיכה ב- WINS או בשמות NetBIOS, ודא שכל המחשבים והתוכנות ברשת שלך מסוגלים לתפקד באמצעות שירות שמות אחר, כגון DNS.
- **האם הרשת שלי היא רשת משנה (Subnet) יחידה, או שהיא מנותבת עם מספר Subnets נוספות?** אם כל הרשת שלך היא בסך הכל רשת LAN זעירה הכוללת מקטע רשת יחיד ובו פחות מ-50 לקוחות, רוב הסיכויים שתסתדר מספיק טוב גם ללא שרת WINS.

שיקולים בנוגע לשרתי WINS

לפני שתיישם את WINS באגד רשתות (Internetwork), שקול את מספר שרתי WINS להם תזדקק. לאגד רשתות דרוש רק שרת WINS אחד, מפני שבקשות להסדרת שמות הן צרורות נתונים ישירים הניתנים לניתוב. שני שרתי WINS מבטיחים מערכת גיבוי לשם עמידות בפני תקלות (Fault Tolerance). אם שרת אחד הופך ללא זמין יכול השרת השני לבצע את פעולת ההסדרה. עליך לשקול את ההמלצות הבאות לגבי שרת WINS :

- לא קיימת מגבלה מובנית למספר בקשות WINS בהן יכול לטפל שרת WINS, אך בדרך כלל הוא יכול לטפל ב- 1500 רישומי שמות ובערך 4500 שאילתות שם בדקה.
- ההמלצה השמרנית היא שרת WINS אחד ושרת גיבוי אחד עבור כל 10,000 לקוחות WINS.
- מחשבים מרובי מעבדים (Multi Processor Systems) הציגו ביצועים טובים יותר בכ- 25% עבור כל מעבד נוסף שהותקן בהם, כאשר מטלה (Thread) WINS נפרדת מופעלת עבור כל אחד מהמעבדים.
- אם רישום שינויים ביומן עבור מסד הנתונים אינו פעיל (באמצעות WINS Manager) רישום שמות מתבצע הרבה יותר מהר, אבל במידה ומתרחשת קריסת מערכת, קיימת סכנה שחלק מהעדכונים האחרונים יאבד.

דרישות WINS

לפני שתתקין את WINS עליך לקבוע שהשרת והלקוחות שלך עומדים בדרישות החומרה. שירות WINS חייב להיות מוגדר בלפחות מחשב אחד באגד רשתות TCP/IP בו פועל Windows NT Server או Windows 2000 Server (הוא אינו חייב להיות Domain Controller). לשרת חייבת להיות כתובת IP, Subnet Mask, Default Gateway ופרמטרים נוספים של TCP/IP. פרמטרים אלה יכולים להיות מוקצים על ידי שרת DHCP, אך מומלץ שהם יוגדרו באופן ידני כהגדרות סטטיות למחשב זה.

לקוח WINS יכול להיות מחשב הפועל בסביבת אחת ממערכות ההפעלה הנתמכות הבאות :

- Windows 2000
- Windows NT גירסה 3.5 או גבוהה יותר
- Windows 95 או Windows 98
- Windows for Workgroups בה מותקן TCP/IP-32
- Microsoft Network Client עבור MS-DOS
- LAN Manager 2.2c עבור MS-DOS

ללקוח חייבת להיות מוגדרת כתובת IP של שרת WINS עיקרי, או של שרת WINS עיקרי ושרת WINS משני.

➢ **כדי להתקין את WINS בשרת מבוסס Windows 2000 Server**

1. בלוח הבקרה לחץ לחיצה כפולה על הסמל Add/Remove Programs.
2. לחץ על Add/Remove Windows Components.

   נפתח חלון Windows Components Wizard.
3. בחלון Windows Components בתיבה Components לחץ על Network Serivces, ולחץ על Details. מופיעה תיבת דו-שיח Network Serivces.
4. סמן את תיבת הסימון Windows Internet Name Service (WINS), לחץ OK, ולחץ Next.

שימוש במיפוי סטטי

ניתן להוסיף ל-WINS רשומות מיפוי שם-לכתובת בשני אופנים:

❖ באופן דינמי, על ידי לקוחות מאופשרי-WINS המתקשרים ישירות עם שרת WINS כדי לרשום, לשחרר או לחדש את שמות NetBIOS שלהם במסד הנתונים של השרת.

❖ באופן ידני, על ידי מנהל מערכת (Administrator) המשתמש ב- WINS MMC או בכלים של שורת הפקודה, כדי להוסיף או למחוק רשומות מיפוי סטטיות במסד הנתונים של השרת.

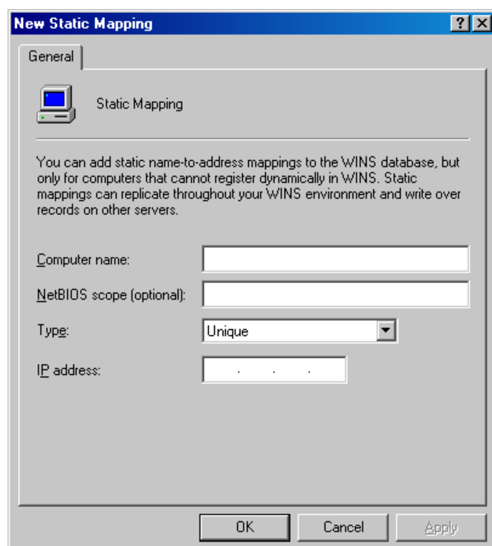
רשומות סטטיות יעילות רק כאשר אתה צריך להוסיף מיפוי שם-לכתובת למסד הנתונים של השרת עבור מחשב שאינו משתמש ב-WINS באופן ישיר. לדוגמה, ברשתות מסוימות שרתים הפועלים בסביבות עבודה אחרות אינם יכולים לרשום שם NetBIOS ישירות לשרת WINS. למרות שניתן להוסיף שמות אלה ולהסדיר אותם באמצעות קובץ LMHOSTS, או על ידי ביצוע שאילתה לשרת DNS, יכול להיות ותשקול את השימוש במיפוי סטטי כתחליף.

➢ **כדי להגדיר מיפוי סטטי**

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ולחץ על WINS.
2. ב- WINS MMC, תחת שרת ה-WINS שלך, לחץ על Active Registrations.
3. פתח את תפריט Action, ובחר New Static Mapping.

   מופיעה תיבת דו-שיח New Static Mapping, כפי שמוצגת בתרשים *9.9*.
4. בשדה Computer Name הקלד את שם NetBIOS של המחשב.
5. בשדה NetBIOS Scope תוכל להקליד את מזהה מרחב NetBIOS (NetBIOS Scope Identifier), אם נעשה בכזה שימוש עבור המחשב. אחרת, השאר שדה זה ריק.
6. בשדה Type בחר באחד מהסוגים הנתמכים כדי לציין האם רשומה זו היא מסוג Unique, Group, Domain Name, Internet או Multihomed, כפי שמפורט בטבלה *9.3*.
7. בשדה IP Address הקלד את כתובתו של מחשב זה.
8. לחץ Apply כדי להוסיף רשומת מיפוי סטטי למסד הנתונים.

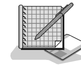
   תוכל להוסיף רשומות מיפוי סטטי נוספות. לחץ על Apply בכל פעם שהשלמת רשומה, ולסיום לחץ על Cancel, כדי לסגור את תיבת הדו-שיח לעריכת המיפויים הסטטיים.
9. לחץ OK כדי לסגור את תיבת דו-שיח New Static Mapping.



תרשים 9.9 תיבת דו-שיח New Static Mapping

טבלה 9.3 סוגי מיפוי סטטי של WINS

סוג	פירוט
Unique	שם ייחודי הממופה לכתובת IP יחידה.
Group	נקרא לעיתים גם Normal Group. כאשר מוסיפים רשומה ל-Group באמצעות WINS Manager, עליך להקליד את שם המחשב וכתובת IP. אבל, כתובות ה-IP של חברים בקבוצה אינן מאוחסנות במסד הנתונים של WINS. מכיון שכתובות החברים בקבוצה אינן מאוחסנות, אין גבול למספר החברים שניתן לצרף לכל קבוצה. כדי לתקשר עם חברי הקבוצה נעשה שימוש במנות שם (Name Packets) המשודרות Broadcast.
Domain Name	מיפוי שם NetBIOS/כתובת IP המקבל את הערך 0x1C בתור הבית ה-16 (16th Byte). המספר המירבי של כתובות אותן ניתן לאחסן ב-Domain Group הוא 25. עבור רישום הכתובת שאחרי העשרים וחמישה, דורס WINS כתובת משוכפלת, או מוחק את הרשומה הישנה ביותר, אם כזו אינה קיימת.
Internet Group	קבוצות אינטרנט הן קבוצות המוגדרות על ידי המשתמש אשר מאפשרות לך לקבץ משאבים, כגון מדפסות, להקלה בתהליך הפנייה או עיון ברשת. בקבוצת אינטרנט (Internet Group) ניתן לאחסן עד 25 כתובות של חברים. אבל, חבר דינמי אינו מחליף חבר סטטי המוסף באמצעות WINS Manager או על ידי יבוא קובץ LMHOSTS.
Multihomed	שם ייחודי (Unique) אשר יכולות להיות משויכות לו יותר מאשר כתובת אחת. הדבר משמש למחשבים בהם מותקן יותר מכרטיס רשת אחד. כל קבוצת Multihomed יכולה לכלול עד 25 כתובות. עבור רישום הכתובת שאחרי העשרים וחמישה, דורס WINS כתובת משוכפלת, או מוחק את הרשומה הישנה ביותר, אם כזו אינה קיימת.



תרגול: הגדרת לקוח WINS

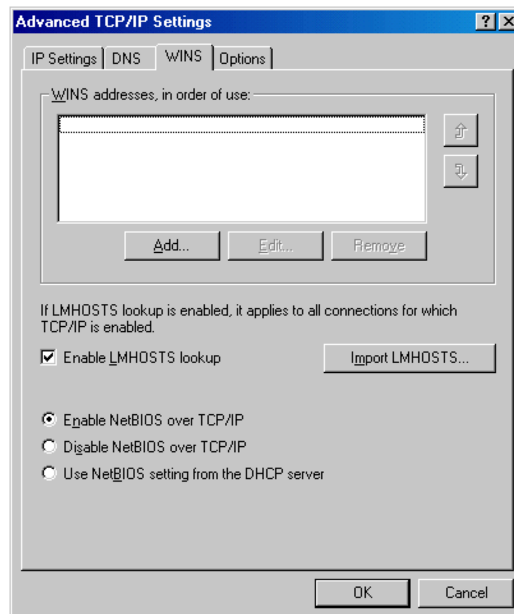
אם מחשב משמש כלקוח DHCP תוכל להגדיר את שרת DHCP כך שיספק ללקוחות DHCP מידע אודות תצורת WINS. לחילופין, תוכל להגדיר את נתוני WINS בלקוחות באופן ידני. אם אתה מגדיר לקוחות WINS באופן ידני עם כתובות ה-IP של אחד או יותר משרתי WINS, ערכים אלה יקבלו קדימות על אותם נתונים המסופקים משרת ה-DHCP.

➢ כדי להגדיר לקוחות WINS באופן ידני עם כתובות ה-IP של אחד או יותר שרתי WINS

1. פתח את חלון Network and Dial-up Connections.
2. לחץ לחיצה ימנית על Local Area Network, ומתפריט הקיצור בחר Properties.

   מופיעה תיבת דו-שיח Local Area Connection Properties.
3. סמן את הרשומה (Internet Protocol (TCP/IP, ולחץ על Properties.

   מופיעה תיבת דו-שיח Internet Protocol (TCP/IP) Properties.
4. לחץ Advanced, ובחר בכרטיסיה WINS Address, כפי שמוצגת בתרשים 9.10.



תרשים 9.10 שירות WINS בלקוח של Windows 2000

5. לחץ ADD. בתיבת דו-שיח TCP/IP WINS Server הקלד את כתובת ה-IP של שרת ה-WINS שלך, ולחץ על ADD.

   תיבת דו-שיח TCP/IP WINS Server תיסגר וכתובת שרת ה-WINS שהקלדת בה תופיע ברשימה שבתיבת דו-שיח Advanced TCP/IP Settings.

6. לחץ OK כדי לסגור את תיבת דו-שיח Advanced TCP/IP Settings.
7. לחץ OK כדי לסגור את תיבת דו-שיח Internet Protocol (TCP/IP) Properties.
8. לחץ OK כדי לסגור את תיבת דו-שיח Local Area Connection Properties.

איתור וטיפול בתקלות WINS

המצבים הבאים עשויים להצביע על בעיה בסיסית ב-WINS :

- מנהל מערכת (Administrator) אינו מסוגל להתחבר ל- WINS MMC.
- שירות TCP/IP NetBIOS Helper בלקוח WINS אינו פעיל (Down) ולא ניתן להפעילו.
- שירות WINS אינו פועל ולא ניתן להפעילו.

הפעולה הראשונה שעליך לנקוט כדי לפתור בעיות WINS היא לוודא שהשירותים המתאימים פעילים. תוכל לעשות זאת הן משרת WINS והן מלקוח WINS.

כדי לוודא שירותים פעילים

1. ודא ששירות WINS פעיל בשרת.
2. ודא שהשירות Workstation, השירות Server והשירות TCP/IP NetBIOS Helper מופעלים (Started) בלקוחות.

אם השירותים אינם מופעלים כהלכה, תוכל להיעזר בכלי הניהול Computer Management כדי לבדוק את עמודת המצב של השירותים, ואז לנסות ולהפעילם באופן ידני. אם לא ניתן להפעיל את השירות, היעזר ב- Event Viewer כדי לבדוק את יומן אירועי המערכת (System Event Log) ולקבוע בעזרתו את הגורם לכשל.

הערה בלקוחות WINS צריכה להופיע המילה Started בעמודה Status **של השירות** TCP/IP NetBIOS Helper. **בשרתי** WINS **צריכה להופיע המילה** Started **בעמודה** Status **של השירות** Windows Internet Name Service (WINS).

הבעיה השכיחה ביותר בלקוחות WINS היא כשל בהסדרת שמות. כאשר מתרחש כשל בהסדרת שמות ענה על השאלות הבאות, כדי לזהות את מקור הבעיה :

- **האם מחשב הלקוח מסוגל להשתמש ב-WINS, והאם הוא מוגדר כהלכה?** ראשית, ודא שהלקוח מוגדר לעבודה עם TCP/IP ועם WINS. ניתן להגדיר תצורת לקוח של הגדרות המשויכות ל-WINS באופן ידני על ידי מנהל מערכת (Administrator) המגדיר את תצורת TCP/IP של הלקוח, או לבצע זאת באופן דינמי על ידי שרת DHCP המספק ללקוח את הגדרות TCP/IP שלו. במקרים רבים, מחשבים בהם פועלות גרסאות ישנות של מערכות ההפעלה של Microsoft מסוגלים להשתמש ב-WINS, לאחר שמותקן ומוגדר בהם TCP/IP. במקרה של Windows 2000, מנהלי מערכת יכולים לבטל (Disable) באופן ידני ויזום את NetBT עבור כל לקוח. אם אתה מבטל את NetBT, לא ניתן להשתמש ב-WINS בלקוח.

הערה אם שרת WINS אינו מגיב לביצוע PING ישיר אליו, קרוב לוודאי ששורש הבעיה טמון בקישוריות רשת בין הלקוח לבין שרת ה-WINS.

- **האם השם שהסדרתו נכשלה היה שם NetBIOS או שם DNS?** שמות NetBIOS מכילים עד 15 תווים, והמבנה שלהם שונה ממבנה שם DNS, שהם בדרך כלל ארוכים יותר ונעשה שימוש בנקודות להפרדה בין כל רמת domain בשם. לדוגמה, ייתכן ששם NetBIOS הקצר PRINT-SRV1 ושם ה-DNS הארוך print-srv1.example.microsoft.com מצביעים שניהם על אותו מחשב משאב הפועל בסביבת Windows 2000 (שרת הדפסה ברשת), המוגדר לשימוש בכל אחד מהשמות. אם נעשה שימוש בשם הקצר בדוגמה הקודמת, Windows 2000 תערב תחילה את שירותי שמות NetBIOS, כגון שידורי WINS או NetBT רחבים, בניסיונותיה הראשונים להסדרת השם. אם בכשל היה מעורב שם ארוך יותר, או כזה בו נעשה שימוש בנקודות, רוב הסיכויים שהסיבה לכישלון בהסדרת השמות נעוצה ב-DNS.

הבעיה השכיחה ביותר בשרת WINS היא חוסר אפשרות להסדיר שמות עבור לקוחותיו. כאשר שרת כושל בהסדרת שמות עבור לקוחותיו, מתגלה התקלה על ידי הלקוחות באחת משתי הדרכים:

- השרת שולח ללקוח תגובה שלילית לשאילתה (Negative Query Response), כגון הודעת שגיאה המציינת Name not found.
- השרת שולח ללקוח תגובה חיובית לשאילתה (Positive Query Response), אך הנתונים שבתגובה אינם נכונים.

אם הגעת לכלל החלטה שמקור הבעיה המשויכת ל-WINS אינו נעוץ בלקוח, ענה על השאלה הבאה, כדי להמשיך בתהליך איתור מקור הבעיה בשרת ה-WINS של אותו לקוח:

- **האם שרת ה-WINS מסוגל לתת את השירות ללקוח?** בשרת ה-WINS של הלקוח שאינו מצליח לאתר שם, היעזר ב- Event Viewer או ב- WINS Management MMC כדי לבדוק אם WINS פעיל כרגע. אם WINS פעיל בשרת, חפש את השם אותו חיפש הלקוח, כדי לראות אם הוא קיים במסד הנתונים.

אם שרת WINS כושל או רושם הודעות שגיאה לגבי שלמות מסד הנתונים, תוכל להיעזר בטכניקות התאוששות מסד הנתונים של WINS תוך שימוש ב- WINS MMC. ראשית, אתה מגדיר תיקיה לגיבוי מסד הנתונים, ואז WINS יפיק גיבויים שלו לתיקיה המוגדרת. כברירת מחדל מבוצע הגיבוי אחת לשלוש שעות. אם מסד נתוני WINS שלך נפגע, תוכל לשחזר אותו בקלות. הדרך הקלה ביותר לשחזור מסד נתונים של שרת מקומי הוא לשכפל את הנתונים חזרה משותף השכפול (Replication Partner) שלך. אם הפגיעה מוגבלת למספר רשומות בלבד, תוכל לתקן אותן על ידי חיוב שכפול של רשומות WINS תקינות. דבר זה יסיר את הרשומות הפגועות גם משרתי WINS אחרים. אם שינויים משוכפלים בין השרתים לעיתים קרובות, הדרך הטובה ביותר לשחזור מסד הנתונים של שרת WINS המקומי היא להשתמש בשותף השכפול, בתנאי שנתוני WINS בשותף השכפול הם המעודכנים יותר.

ניהול וניטור WINS

WINS MMC משתלב במלואו ב- MMC, סביבת עבודה בעלת עוצמה ויחד עם זאת ידידותית למשתמש, אותה תוכל להתאים כך שתהיה יעילה לצרכיך. מכיון שכל כלי ניהול השרת הנכללים לשימושך יחד עם Windows 2000 Server מהווים חלק מ-MMC, תוכניות שירות מבוססות-MMC קלות יותר לשימוש, מפני שהן מתפקדות באופן צפוי ועיצובן דומה. יתר על כן, תכונות מתקדמות מסוימות של WINS בגרסאותיו הישנות יותר, שהיוו חלק משרת Windows NT ואשר ניתן היה להגדירן רק מתוך רישום המערכת (Registry), ניתנות היום לגישה ישירה וקלה יותר. מתוך תכונות אלו ניתן למנות בין השאר את האפשרות לחסום רשומות בפני בעלים מסוים או שותף שכפול (היה ידוע בעבר כ- Persona Non Grata) או האפשרות לאפשר אכיפה של מיפוי סטטי (היה ידוע בעבר כ- Migrate On/Off). בשיעור זה תלמד כיצד לנהל ולנטר את WINS באמצעות WINS MMC.

צפייה בסטטיסטיקות של שרת WINS

עליך לצפות מדי פעם בסטטיסטיקות של שרת WINS כדי לנטר את ביצועיו. כברירת מחדל, מתעדכנים הנתונים הסטטיסטיים מדי 10 דקות. תוכל גם, אם תרצה, לבטל אפשרות זו על ידי ביטול הסימון ליד Automatically Update Statistics Every.

➢ כדי לפתוח את תיבת דו-שיח WINS Server Statistics

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ולחץ על WINS.
2. ב- MMC Tree לחץ על שרת WINS הרצוי.
3. פתח את תפריט Action ובחר Display Server Statistics.
4. כדי לעדכן את התצוגה תוך כדי הצפיה בסטטיסטיקות WINS, לחץ Refresh.

סיכום שיעור

כדי ליישם את WINS יש להגדיר נכון, הן את הלקוח והן את השרת. הגדרת מיפוי סטטי עבור לקוחות שאינם לקוחות-WINS, מאפשר ללקוחות WINS ברשתות מרוחקות לתקשר עימם. כאשר מנסים לאתר תקלה ב-WINS, הפעולה הראשונה בה יש לנקוט היא לוודא שהשירותים הנדרשים אכן פעילים.

שיעור 4: הגדרת שכפול WINS

כל שרתי WINS באגד רשתות (Internetwork) יכולים להיות מוגדרים לביצוע שכפול מלא של רשומות מסדי הנתונים עם שרתי WINS אחרים. דבר זה מבטיח ששם הרשום בשרת WINS אחד ישוכפל בסופו של דבר לכל שרתי WINS האחרים. שיעור זה מסביר כיצד משוכפלות רשומות מסדי הנתונים של WINS לשרתי WINS אחרים.

לאחר שיעור זה, תוכל

- להוסיף שותף שכפול.
- לבצע שכפול מסד נתוני WINS.

זמן לימוד משוער: 20 דקות

סקירת השכפול

שכפול מסד נתונים (Database Replication) מתרחש בכל פעם שמסד הנתונים משתנה, כולל כאשר שם משוחרר. שכפול מסדי נתונים מאפשר לשרת WINS להסדיר שמות NetBIOS של מארחים הרשומים עם שרת WINS שונה. לדוגמה, אם מארח ברשת משנה 1 רשום בשרת WINS באותה רשת משנה, אבל מעוניין לתקשר עם מארח ברשת משנה 2, ומארח זה רשום בשרת WINS שונה, לא ניתן יהיה להסדיר את שם ה-NetBIOS אלא אם שני שרתי ה-WINS משכפלים את מסדי הנתונים שלהם אחד עם השני.

כדי לשכפל רשומות מסד נתונים, חייב כל שרת WINS להיות מוגדר כשותף מושך (Pull Partner) או כשותף דוחף (Push Partner) עם לפחות שרת WINS אחד אחר. שותף דוחף הוא שרת WINS השולח הודעה לשותפים המושכים שלו, ומיידע אותם כאשר התרחשו שינויים במסד נתוני WINS. כאשר השותפים המושכים של שרת WINS מגיבים להודעה באמצעות בקשה לשכפול (Replication Request), שולח שרת ה-WINS עותק של רשומות מסד הנתונים החדשות (שכפול שלהן) לשותפים המושכים שלו.

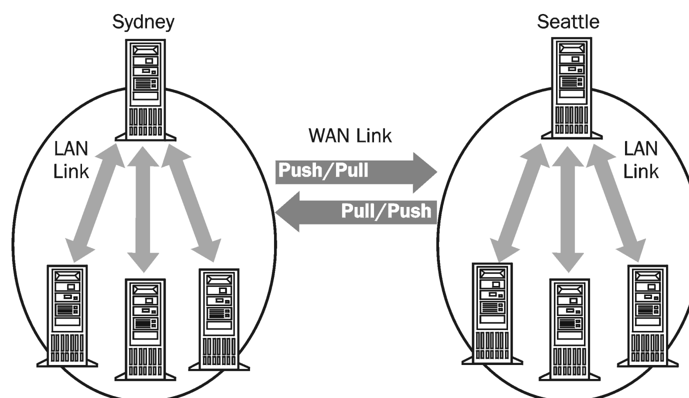
שותף מושך הוא שרת WINS המבקש רשומות מסד נתונים חדשות (שכפול שלהן) מהשותפים הדוחפים שלו. הדבר מתבצע באמצעות בקשת הרשומות להן מספר גירסה גבוה יותר ממספר הגירסה שסופק לו בעת ביצוע השכפול האחרון.

הערה שרתי WINS משכפלים רק רשומות חדשות במסד הנתונים שלהם. מסד נתוני WINS השלם אינו משוכפל בכל פעם שמתבצע שכפול.

הגדרת שרת WINS כשותף דוחף או מושך

ההחלטה אם לקבוע את שרת WINS כשותף דוחף או כשותף מושך תלויה בסביבת הרשת שלך. זכור את הכללים הבאים (מתוארים בתרשים 9.11) כאשר אתה מגדיר שכפול של שרת WINS :

- ❖ הגדר שותף דוחף (Push Partner) כאשר השרתים מחוברים בקישורים מהירים, מפני ששכפול בדחיפה מתרחש כאשר התבצע מספר מוגדר של שינויים ברשומות במסד נתוני WINS.



תרשים 9.11 הגדרות שותף דוחף ושותף מושך

- ❖ הגדר שותף מושך (Pull Partner) בין אתרים (Sites), ובמיוחד כאשר מדובר בקישורים איטיים, מפני שניתן להגדיר ששכפולים במשיכה יתבצעו במרווחי זמן קבועים.
- ❖ הגדר כל שרת שיהיה גם שותף דוחף וגם שותף מושך, כך שישכפלו רשומות מסד נתונים ביניהם.

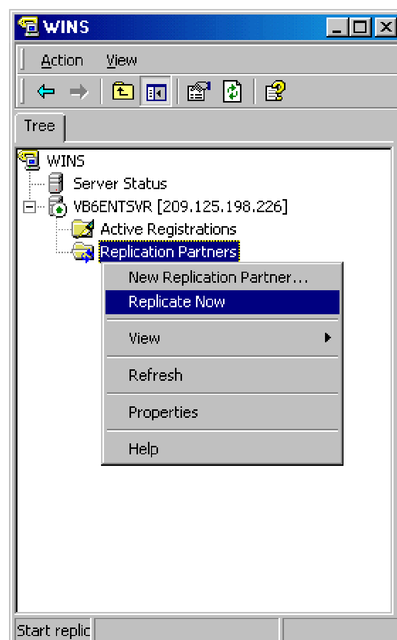
הערה את הגדרת שרת WINS כשותף דוחף או כשותף מושך יש לבצע באמצעות כלי הניהול של WINS.

- ❖ גם בסידני וגם בסיאטל (ראה תרשים 9.11), כל שרתי ה-WINS בכל אתר מושכים את רשומות מסד הנתונים החדשות שלהם משרת יחיד באתר.
- ❖ השרתים המקבלים את השכפול בדחיפה מוגדרים ביניהם לשכפול במשיכה, מפני שקישור הרשת בין סידני לסיאטל הוא איטי למדי. שכפול אמור להתבצע כאשר נעשה הכי פחות שימוש בקישור, למשל מאוחר בלילה.

הגדרת שכפול מסד נתונים

שכפול מסד נתונים (Database Replication) דורש שתגדיר לפחות שותף דוחף אחד ושותף מושך אחד. קיימות ארבע שיטות להתחלת שכפול מסד נתוני WINS:

1. כשהמערכת מופעלת. כברירת מחדל, לאחר ששותף השכפול מוגדר, יוזם WINS באופן אוטומטי שכפול במשיכה (Pull) של רשומות מסד נתונים בכל פעם ש-WINS מופעל. שרת WINS יכול גם להיות מוגדר לדחיפה (Push) בעת הפעלת המערכת.
2. במרווחי זמן מוגדרים, למשל כל חמש שעות.
3. כאשר שרת WINS הגיע לסף מוגדר של מספר רישומים ושינויים למסד נתוני WINS. כאשר מגיע הסף (הגדרת מונה העדכונים) מיידע שרת WINS את כל שותפי המשיכה שלו, אשר כתגובה יגישו בקשה לקבל את הרשומות החדשות.
4. על ידי חיוב שכפול מתוך WINS MMC, כפי שמוצג בתרשים 9.12.



תרשים 9.12 חיוב ביצוע שכפול מסד נתוני WINS

תרגול: שכפול מסד נתוני WINS

בהליכים אלה תגדיר את שרת WINS שלך לבצע שכפול מסדי נתונים עם שרת WINS אחר.

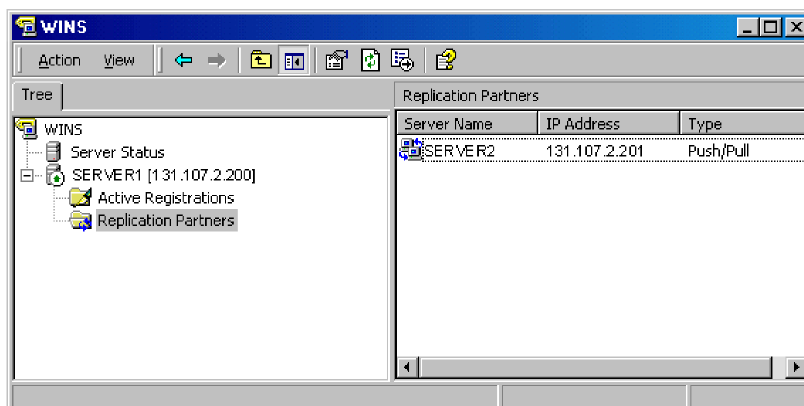
הערה כדי להשלים הליך זה, עליך קודם כל להגדיר את המחשב האחר שלך (Server2) כשרת WINS.

➤ כדי להגדיר שותפים לשכפול WINS

1. פתח את WINS MMC.
2. לחץ לחיצה ימנית על התיקיה Replication Partners שתחת שרת ה-WINS שלך, ובחר New Replication Partner.

   מופיעה תיבת דו-שיח New Replication Partners.
3. בשדה WINS Server, הקלד כתובת IP של שרת WINS השותף ולחץ OK.

   מופיעה תיבת דו-שיח Replication Partners וכתובת ה-IP שלך נוספת ברשימת שרתי WINS, כפי שנראה בתרשים 9.13.



תרשים 9.13 שותפי שכפול הרשומים ב- WINS MMC

4. לחץ לחיצה ימנית על שותף השכפול שזה עתה יצרת בחלונית הימנית, ומתפריט הקיצור בחר Properties.

   מופיעה תיבת דו-שיח Server Properties.

5. בחר בכרטיסיה Advanced.
6. מתיבת הרשימה הנפתחת Replication Partner Type בחר באפשרות Pull.
7. מרווח הזמן לשכפול נקבע על 30 דקות.
8. לחץ OK.

בהליך זה תאכוף על WINS לבצע את מסד נתוני WINS עם שרת WINS.

כדי לאכוף ביצוע שכפול

1. לחץ לחיצה ימנית על התיקיה Replication Partner.
2. מתפריט הקיצור בחר Replicate Now.

   מופיעה תיבת דו-שיח בה אתה נשאל אם אתה בטוח שברצונך להתחיל בשכפול.

3. לחץ Yes.

   מופיעה תיבת הודעה המציינת שבקשה לשכפול נשלחה לתור ההודעות (Queued).

4. לחץ OK.

תכנון מספר שרתי WINS בהם ייעשה שימוש

ברשתות קטנות, מסוגל שרת WINS יחיד לשרת בקשות להסדרת שמות NetBIOS מאת כ- 10,000 לקוחות. כדי לספק עמידות נוספת בפני תקלות (Fault Tolerance) תוכל להגדיר מחשב נוסף בו פועלת מערכת ההפעלה Windows 2000 Server כשרת WINS גיבוי עבור הלקוחות. אם אתה משתמש רק בשני שרתי WINS תוכל להגדירם בקלות כשותפי שכפול אחד של השני. לשכפול פשוט בין שני השרתים, אחד צריך להיות מוגדר

כשותף הדוחף והשני צריך להיות מוגדר כשותף המושך. השכפול יכול להתבצע באופן ידני, או באופן אוטומטי, מה שתוכל להגדיר על ידי סימון תיבת הסימון Enable Automatic Partner Configuration, בכרטיסיה Advanced שבתיבת דו-שיח Partnet Properties.

רשתות גדולות יותר דורשות לעיתים מספר גדול יותר של שרתי WINS ממספר סיבות, כשהחשובה מביניהן היא מספר חיבורי הלקוחות לכל שרת. מספר המשתמשים בהם יכול שרת WINS לתמוך משתנה בהתאם לדפוסי השימוש, אחסון המידע ואפשרויות העיבוד של המחשב שרת WINS. סביבות רשת ארגוניות מסוימות דורשות חומרה עתירת ביצועים וחזקה הרבה יותר כדי לבצע פעילות WINS, כך שייתכן שתרוויח משדרוג מחשב השרת. כאשר אתה מתכנן את השרתים שלך, זכור שכל שרת WINS יכול לטפל במאות רישומים ושאילתות בכל שנייה. למטרות עמידות בפני תקלות ניתן להשתמש במספר כלשהו של שרתים. אבל, עליך להימנע מלהגדיר מספר גדול מדי של שרתי WINS, אלא אם הם באמת נחוצים. על ידי הגבלת מספר שרתי WINS ברשת שלך, אתה מפחית את התעבורה הנגרמת כתוצאה מהשכפולים, מספק הסדרת שמות NetBIOS יעילה יותר ומפחית את הדרישות הניהוליות.

שותפי שכפול אוטומטיים של WINS

אם הרשת שלך תומכת בשידור מרובה (Multicasting), יכול שרת WINS להיות מוגדר כך שיאתר באופן אוטומטי שרתי WINS אחרים ברשת על ידי שידור מרובה לכתובת IP 224.0.1.24. כברירת מחדל, מתרחש שידור מרובה זה כל 40 דקות. כל שרתי ה-WINS שאותרו ברשת מוגדרים באופן אוטומטי כשותפי שכפול דוחפים/מושכים (Push/Pull), כאשר שכפול במשיכה מוגדר להתרחש בכל שעתיים. אם נתבי רשת אינם תומכים בשידור מרובה ימצא שרת ה-WINS רק שרתי WINS אחרים באותה רשת משנה (Subnet). כברירת מחדל, שותפויות אוטומטיות בין שרתי WINS אינן פעילות. כדי לבטל אפשרות זו באופן ידני, היעזר בעורך הרישום (Registry Editor) ושנה את ערך המפתח UseSelfFndPnrs ל-0 (אפס) ואת ערך המפתח McastIntvl לערך גבוה.

גיבוי מסד הנתונים של WINS

WINS MMC מספק כלים לגיבוי, כדי שתוכל לגבות ולשחזר את מסד נתוני WINS. כאשר WINS מגבה את מסד הנתונים מהשרת, הוא יוצר את התיקיה \Wins_bak\New תחת תיקיית הגיבוי שהוגדרה על ידך כנתיב ברירת המחדל (Default) לגיבוי בתיבת דו-שיח Server Properties. הגיבויים עצמם של מסד נתוני WINS (קבצי WINS.MDB) מאוחסנים בתיקיה זו. כברירת מחדל, נתיב הגיבוי הוא תיקיית השורש (Root Folder) של מחיצת המערכת שלך, למשל \:C. לאחר שתציין תיקיית גיבוי עבור מסד הנתונים שלך, מבצע WINS גיבוי מלא של הקבצים אחת לשלוש שעות, תוך שימוש בתיקיה המוגדרת. ניתן גם להגדיר את WINSS כך שייגבה את מסד הנתונים באופן אוטומטי, כאשר השירות מופסק או כאשר מחשב השרת מכובה.

➤ **כדי לגבות מסד נתוני WINS**

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ובחר WINS.
2. ב-Console tree לחץ על שרת ה-WINS הרצוי.
3. פתח את תפריט Action ובחר Backup Database.
4. כאשר תתבקש לאשר, לחץ Yes.
5. לאחר שתהליך הגיבוי מסתיים, לחץ OK.

חשוב אל תציין כונן רשת כמיקום הגיבוי. בנוסף, אם אתה משנה את הנתיב של גיבוי WINS או של מסד הנתונים שלו במאפייני השרת (Server Properties), בצע גיבוי חדש כדי להבטיח שחזורים מוצלחים בעתיד של מסד נתוני WINS. זוהי הדרך היחידה בה מגובה מסד נתוני WINS הפעיל, מפני שמסד הנתונים נעול כשהוא פתוח, כל עוד שרת WINS פעיל.

סיכום שיעור

כל שרתי WINS ברשת נתונה יכולים להיות מוגדרים כך שיתקשרו בינם לבין עצמם, כך ששם שנרשם באחד מהם יהיה ידוע בסופו של דבר לכל שרתי WINS ברשת. שותף מושך (Pull Partner) מבקש רשומות מסד נתוני WINS חדשות. שותף דוחף (Push Partner) שולח הודעה לשותפים המושכים שלו ומיידע אותם שמסד נתוני WINS שלו השתנה.

שאלות סיכום

השאלות הבאות נועדו לחזק את הנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות על שאלה, עיין בשיעור המתאים ונסה את השאלה שנית. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואחר כך בעברית.

Answering the following questions will reinforce key information presented in this chapter. If you are unable to answer a question, review the appropriate lesson and then try the question again. Answers to the questions can be found in Appendix A, "Questions and Answers".

1. What are two benefits of WINS?
2. What two methods can be used to enable WINS on a client computer?
3. How many WINS servers are required in an intranet of 12 subnets?
4. What types of names are stored in the WINS database?

1. מנה שני יתרונות לשימוש ב-WINS.
2. באיזה שתי שיטות ניתן להשתמש כדי לאפשר את WINS במחשב לקוח?
3. כמה שרתי WINS דרושים לרשת אינטראנט ובה 12 Subnets?
4. איזה סוגי שמות מאוחסנים במסד הנתונים של WINS?

פרק 10

יישום DHCP
(Dynamic Host Configuration Protocol)

אודות פרק זה

בפרק זה תלמד כיצד להשתמש ב-DHCP (Dynamic Host Configuration Protocol) כדי להגדיר באופן ידני את TCP/IP (Transmission Control Protocol/Internet Protocol) ולמנוע על ידי כך שגיאות הגדרה נפוצות. במשך השיעור תתקין ותגדיר שרת DHCP, תבחן את הגדרות DHCP, ואז תשיג כתובות IP משרת DHCP.

לפני שתתחיל

להשלמת פרק זה צריך שיהיה ברשותך:

- מחשב בו מותקנת מערכת ההפעלה Windows 2000 Server, ובה מוגדר פרוטוקול TCP/IP.

שיעור 1: הכרת DHCP והתקנתו

DHCP מקצה באופן אוטומטי כתובות IP למחשבים. DHCP מתגבר על מגבלות ההגדרה הידנית של TCP/IP. שיעור זה יסקור את DHCP וכיצד הוא פועל.

לאחר שיעור זה, תוכל

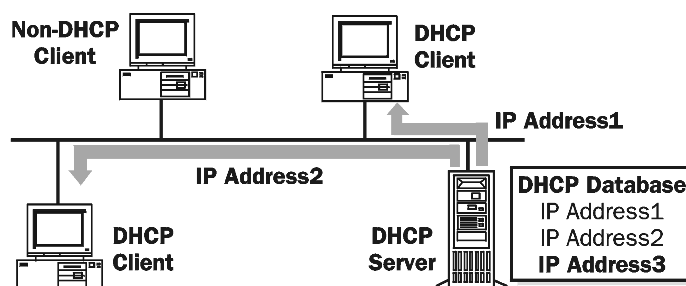
- לתאר את ההבדל בין הגדרה ידנית להגדרה אוטומטית של TCP/IP.
- לזהות פרמטרים של הגדרות TCP/IP **אותן ניתן להחיל באמצעות** שרת DHCP.
- לתאר **את** IP Lease Request **ואת** IP Lease Offer.
- להתקין **את** DHCP במחשב Windows 2000.

זמן לימוד משוער: 20 דקות

סקירת DHCP

DHCP הוא הרחבה של פרוטוקול BOOT (BOOTP). BOOTP מאפשר ללקוחות Diskless (כאלה שלא מותקן בהם כונן דיסק קשיח המאפשר את הפעלת המחשב באופן מקומי) להיות מופעלים ולקבל באופן אוטומטי הגדרות TCP/IP. DHCP מרכז ומנהל את שיוך נתוני הגדרות TCP/IP על ידי הקצאה אוטומטית של כתובות IP למחשבים המוגדרים לשימוש ב-DHCP. יישום DHCP מפחית את כמות תקלות ההגדרה הנובעות מהגדרת TCP/IP באופן ידני.

כפי שמתואר בתרשים 10.1, בכל פעם שלקוח DHCP מופעל הוא מבקש את נתוני מיעון IP משרת DHCP. נתונים אלה כוללים את כתובת ה-IP, Subnet Mask וערכים אופציונליים נוספים. הערכים האופציונליים עשויים לכלול כתובת Default Gateway, כתובת שרת DNS (**D**ynamic **N**ame **S**ystem) וכתובת שרת WINS (**W**indows **I**nternet **N**ame **S**ervice).



תרשים 10.1 כיצד מתקשר לקוח DHCP עם שרת DHCP

כאשר שרת DHCP מקבל בקשה הוא בוחר נתוני מיעון IP מתוך מאגר כתובות המוגדר במסד הנתונים שלו, ומציע אותם ללקוח DHCP. אם הלקוח מקבל את ההצעה, מוחכרים נתוני מיעון ה-IP ללקוח למשך זמן מוגדר. אם לא קיימים במאגר נתוני מיעון IP זמינים להחכרה ללקוח, הלקוח אינו יכול לאתחל את TCP/IP.

הגדרה ידנית מול הגדרה אוטומטית

כדי להבין מדוע DHCP הוא יעיל בהגדרת TCP/IP במחשבי לקוח, רצוי להעמיד את השיטה הידנית להגדרת TCP/IP מול השיטה האוטומטית הנעזרת ב-DHCP.

הגדרה ידנית של TCP/IP

הכוונה בהגדרה ידנית של TCP/IP היא שהמשתמשים יכולים לבחור כך סתם בכתובת IP אקראית, במקום לקבל כתובת IP חוקית ממנהל הרשת. השימוש בכתובת IP שאינה נכונה עלול לגרום לתקלות רשת שקשה מאוד יהיה לעלות על מקורן.

בנוסף, הקלדת כתובת IP, Subnet Mask או Default Gateway עלולה לגרום לתקלות, החל בבעיות התחברות אם הגדרות ה- Default Gateway או ה- Subnet Mask שגויות, וכלה בכפילויות של כתובות IP.

מגבלה אחרת של הגדרה ידנית של TCP/IP היא העומס שבניהול אגד רשתות (Internetwork), בהן מחשבים מועברים לעיתים קרובות למדי מרשת משנה אחת לאחרת. למשל, כאשר תחנת עבודה מועברת ל-Subnet אחרת, כתובת ה-IP וכתובת שער ברירת המחדל שלה חייבים להשתנות, כדי שתחנה זו תוכל לתקשר ממיקומה החדש.

הגדרת TCP/IP באמצעות DHCP

כאשר נעשה שימוש ב-DHCP כדי להגדיר באופן אוטומטי את נתוני מיעון IP, המשתמשים כבר אינם צריכים להשיג את נתוני מיעון IP ממנהל הרשת כדי להגדיר את TCP/IP. שרת DHCP מספק את כל נתוני ההגדרות הדרושים לכל לקוחות DHCP. רבות מבעיות הרשת הקשות יותר לאיתור נעלמות בעת השימוש ב-DHCP.

פרמטרים בהגדרת TCP/IP אשר יכולים להיות מוגדרים באמצעות DHCP כוללים :

- כתובת IP לכל מתאם רשת במחשב הלקוח.
- Sונמקא Mשדל המשמשת לזיהוי חלק רשת ה-IP מחלק המארח בכתובת IP.
- Default Gateways, נתבים, המשמשים לקישור מקטע רשת אחד לאחרים.
- פרמטרים נוספים להגדרה אשר ניתן להגדיר אותם בלקוחות DHCP, אם נמצא הצורך לכך. לדוגמה, כתובות IP של שרתי DNS או WINS בהם יכול הלקוח להשתמש.

כיצד פועל DHCP

DHCP משתמש בתהליך בן ארבעה שלבים כדי להגדיר לקוח DHCP, כפי שמתואר בטבלה 10.1. אם במחשב אחד מותקן יותר ממתאם רשת אחד, מתבצע תהליך DHCP בנפרד עבור כל מתאם רשת המותקן בו. כל תקשורות DHCP מתבצעת באמצעות UDP (**U**ser **D**atagram **P**rotocol) ביציאות (Ports) 67 ו-68.

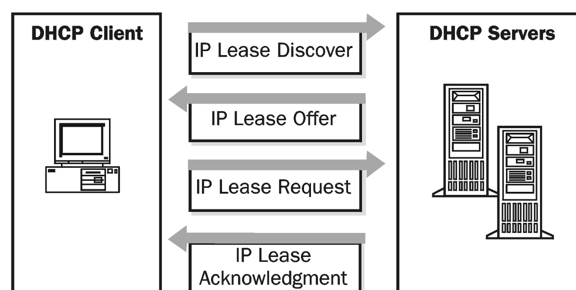
רוב הודעות DHCP נשלחות באמצעות שידור רחב (Broadcast). כדי שלקוחות DHCP יוכלו לתקשר עם שרת DHCP הנמצא ברשת מרוחקת, חייבים הנתבים (Routers) לתמוך בהעברת שידורי DHCP. שלבי הגדרת DHCP מתוארים בטבלה 10.1.

טבלה 10.1 ארבעת השלבים להגדרת לקוח DHCP

שלב	תיאור
גילוי חוזה חכירת IP	הלקוח מאתחל גירסה מצומצמת של TCP/IP ומשדר בקשה לקבל את מיקומו של שרת DHCP ונתוני מיעון IP.
הצעה לחכירת IP	כל שרתי ה-DHCP להם יש נתוני מיעון IP זמינים שולחים ללקוח הצעה.
בקשה לחכירת IP	הלקוח בוחר את נתוני מיעון ה-IP מההצעה הראשונה שהוא מקבל ומשדר הודעה בה הוא מבקש לחכור את נתוני מיעון ה-IP המוצעים לו.
אישור חכירת IP	שרת DHCP שהציע את ההצעה מגיב להודעה וכל שרתי ה-DHCP האחרים מושכים את הצעותיהם. נתוני מיעון ה-IP מוקצים ללקוח ונשלחת הודעת אישור (Acknowledgement). הלקוח מסיים את אתחול ואיגוד (Binding) TCP/IP. לאחר שהושלם תהליך ההגדרה האוטומטי יכול המשתמש להשתמש בכל השירותים ותוכניות השירות של TCP/IP, להתקשרויות רשת רגילות וחיבוריות למארחי IP אחרים.

גילוי והצעת חוזה חכירת IP

כפי שמתואר בתרשים 10.2, בשני השלבים הראשונים מבצע הלקוח שידור רחב לאיתור שרת DHCP, ושרת DHCP מציע כתובת IP ללקוח.



תרשים 10.2 גילוי והצעת חוזה חכירת IP

גילוי חוזה חכירת IP

בעת תהליך האתחול של הלקוח הוא מבקש לחכור כתובת IP, הוא עושה זאת על ידי שידור רחב (Broadcasting) של הבקשה לכל שרתי DHCP. מכיוון שללקוח אין כתובת IP והוא אינו יודע את כתובת ה-IP של שרת DHCP, הוא משתמש בכתובת 0.0.0.0 ככתובת המקור ובכתובת 255.255.255.255 ככתובת היעד.

בקשת החכירה נשלחת בהודעת DHCPDISCOVER. הודעה זו מכילה גם את כתובת החומרה של מחשב הלקוח ואת שם המחשב, כדי ששרתי DHCP ידעו מיהו הלקוח ששלח את הבקשה.

תהליך חכירת IP מתרחש כאשר מתקיים אחד מהתנאים הבאים:

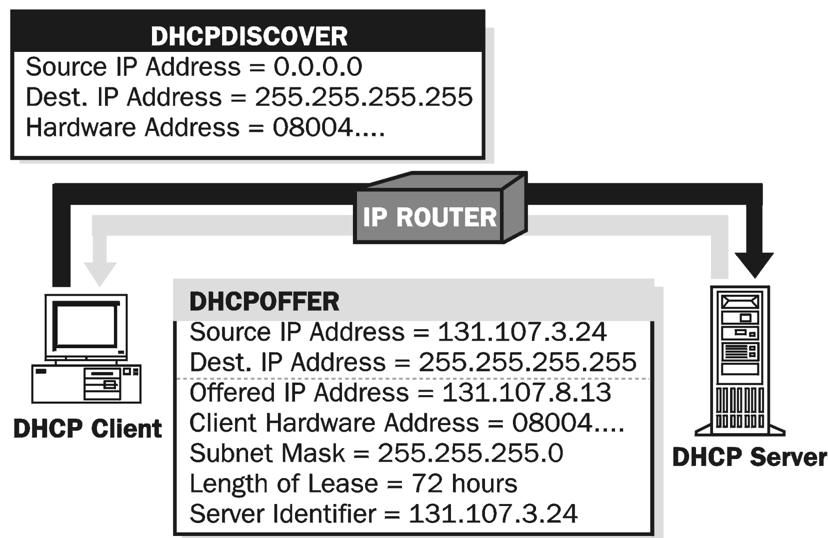
- TCP/IP מאותחל בפעם הראשונה כלקוח DHCP.
- הלקוח מבקש כתובת IP מסוימת והבקשה נדחית, רוב הסיכויים שהדבר קורה מפני ששרת DHCP הפסיק את חוזה החכירה לכתובת זו.
- הלקוח חכר כתובת IP בעבר, אך שחרר אותה וכעת מבקש חוזה חכירה חדש.

הצעת חכירת IP

כל שרתי DHCP המקבלים את הבקשה ויש להם הגדרות חוקיות ללקוח משדרים הצעה הכוללת את המידע הבא:

- כתובת החומרה של הלקוח
- כתובת IP מוצעת
- Subnet Mask
- תוקף חוזה החכירה
- מזהה שרת (Server Identifier, כתובת IP של שרת DHCP מגיש ההצעה)

השימוש ב-Broadcast (שידור רחב) נעשה מפני שללקוח עדיין אין כתובת IP. כפי שמתואר בתרשים 10.3 ההצעה משודרת כהודעת DHCPOFFER. שרת ה-DHCP שומר את כתובת ה-IP המוצעת, כדי שלא תוצע ללקוח DHCP אחר. לקוח ה-DHCP בוחר את כתובת ה-IP המוצעת בהצעה הראשונה שהוא מקבל.



תרשים 10.3 שליחת הודעת DHCPOFFER

כאשר אין שרת DHCP זמין

לקוח DHCP ממתין שנייה אחת להצעה. אם לא התקבלה הצעה לא יוכל הלקוח להיות מאותחל כהלכה, והוא ישוב וישדר שלוש פעמים (במרווחי זמן של 9, 13 ו-16 שניות, ועוד פרק זמן אקראי שבין 0 ל-1000 אלפיות השנייה). אם לאחר ארבע בקשות לא התקבלה הצעה, ינסה הלקוח פעם נוספת מדי חמש דקות.

לקוחות מבוססי-Windows 2000 יכולים להגדיר באופן אוטומטי כתובת IP ו-Subnet Mask, במידה ואין שרת DHCP זמין בעת הפעלת המערכת. זוהי תכונה חדשה של Windows 2000, הנקראת APIPA (**A**utomatic **P**rivate **IP A**ddressing). תכונה זו יעילה עבור לקוחות ברשתות פרטיות קטנות, כגון משרדים קטנים, משרדים ביתיים או לקוחות גישה מרחוק. שירות הלקוח DHCP של Windows 2000 עובר את התהליך הבא כדי להגדיר את הלקוח באופן אוטומטי (Autoconfigure) :

1. לקוח DHCP מנסה לאתר שרת DHCP ולהשיג ממנו כתובת והגדרות תצורה.
2. אם לא ניתן לאתר שרת DHCP, או שהוא אינו מגיב, לקוח ה-DHCP מגדיר באופן אוטומטי את כתובת ה-IP ואת ה- Subnet Mask שלו, תוך שימוש בכתובת נבחרת מרשת Class-B של Microsoft, שכתובתה 169.254.0.0 עם Subnet Mask 255.255.0.0.

   לקוח DHCP בודק אם מתרחשת התנגשות, כדי לוודא שכתובת ה-IP שבחר לא נמצאת כרגע בשימוש ברשת. אם נמצאה התנגשות, בוחר הלקוח כתובת IP אחרת. הלקוח ימשיך לנסות להגדיר את עצמו באופן אוטומטי באופן זה עד לניסוי 10 כתובות.
3. לאחר שהלקוח מצליח למצוא לעצמו כתובת הוא מגדיר את ממשק הרשת שלו לשימוש עם כתובת זו. אז ברקע, ממשיך הלקוח לנסות ולאתר את שרת ה-DHCP כל חמש דקות. אם בשלב מאוחר יותר נמצא שרת DHCP, הלקוח מוותר על הנתונים שהוגדרו בו באופן אוטומטי. כעת ישתמש הלקוח בכתובת המוצעת לו על ידי שרת ה-DHCP (ובכל יתר הפרטים שמגדיר שרת ה-DHCP) כדי לעדכן את הגדרות תצורת IP שלו.

בקשה לחכירת IP ואישור חכירת IP

בשני השלבים האחרונים בוחר הלקוח הצעה ושרת ה-DHCP מאשר את חוזה החכירה.

בקשה לחכירת IP

אחרי שהלקוח מקבל הצעה משרת DHCP אחד לפחות הוא משדר לכל שרתי ה-DHCP כי הוא ביצע בחירה על ידי קבלת הצעה.

שידור זה נשלח בהודעת DHCPREQUEST הכוללת את מזהה השרת (כתובת IP) של השרת שהצעתו התקבלה. כל יתר השרתים מושכים את הצעותיהם, כך שכתובות ה-IP שהם הציעו תהיינה זמינות לבקשת החכירה הבאה.

אישור חכירת IP (מוצלח)

שרת ה-DHCP שהצעתו התקבלה משדר ללקוח הודעת DHCPACK (Successful Acknowledgement), שהוא אישור הצלחה. הודעה זו מכילה חוזה חכירה חוקי לכתובת IP, וייתכן שגם נתוני תצורה נוספים. כאשר הלקוח מקבל את האישור, מאותחל TCP/IP עד תום והוא נחשב מאוגד (Bound) ללקוח DHCP. מרגע שאוגד, יכול הלקוח להשתמש ב-TCP/IP כדי לתקשר באגד הרשתות.

אישור חכירת IP (כושל)

שידור אישור לא מוצלח (DHCPNACK) מתבצע במידה ולקוח מנסה לחכור את כתובת ה-IP הקודמת שלו, וזו כבר אינה זמינה. הוא מופק גם במקרה כתובת ה-IP אינה חוקית, מפני שהלקוח הועבר פיסית ל-Subnet אחרת. כאשר הלקוח מקבל הודעת כשל (Unsuccessful Acknowledgement) הוא שב ומבצע את תהליך בקשת חוזה חכירה לכתובת IP.

התקנת שרת DHCP

לפני שתתקין את שרת DHCP, עליך לזהות את הדברים הבאים :

- ❖ דרישות החומרה ונפח האחסון של שרת DHCP.
- ❖ איזה מחשבים אתה יכול להגדיר מייד כלקוחות DHCP עבור הגדרה דינמית של תצורת TCP/IP ואיזה מחשבים עליך להגדיר באופן ידני עם פרמטרי TCP/IP סטטיים, כולל כתובות IP קבועות.
- ❖ סוגי אפשרויות DHCP והערכים שלהן, אותם יש להגדיר מראש בלקוחות DHCP.

לפני שתתקין את DHCP ענה על השאלות הבאות :

- ❖ **האם כל המחשבים יהפכו להיות לקוחות DHCP?** אם לא, קח בחשבון שללקוחות שהם אינם לקוחות DHCP יש כתובות IP קבועות (סטטיות) וכי יש להוציא את הכתובות הקבועות מטווח הכתובות המוגדר בשרת ה-DHCP. אם לקוח מבקש כתובת IP מסוימת, כתובת זו אמורה להיות שמורה.
- ❖ **האם שרת ה-DHCP יספק כתובות IP למספר Subnets?** אם כן, קח בחשבון שכל הנתבים המקשרים בין רשתות המשנה מתפקדים גם כסוכני ממסר DHCP (DHCP Relay Agent). אם הנתבים שלך אינם מתפקדים כסוכני ממסר DHCP, דרוש לפחות שרת DHCP אחד בכל רשת משנה בה יש לקוחות DHCP. שרת ה-DHCP צריך להוות סוכן ממסר DHCP או נתב בו BOOTP מאופשר.
- ❖ **כמה שרתי DHCP נדרשים?** קח בחשבון ששרת DHCP אינו משתף מידע עם שרתי DHCP אחרים. בשל כך, יש צורך ליצור טווח כתובות IP ייחודי שיסופק על ידי כל שרת ללקוחותיו.

❖ **איזה אפשרויות מיעון IP יקבלו הלקוחות משרת ה-DHCP?** אפשרויות מיעון IP (IP Addressing) קובעות כיצד יש להגדיר את שרת ה-DHCP, והאם יש ליצור את האפשרויות עבור כל הלקוחות באגד הרשתות, ללקוחות ברשת משנה מסוימת או ללקוחות יחידים. אפשרויות מיעון IP כוללות:

- שער ברירת מחדל (Default Gateway)
- שרת DNS
- הסדרת שמות NetBIOS over TCP/IP
- שרת WINS
- מזהה טווח NetBIOS (NetBIOS scope ID)

כדי להתקין שרת DHCP

1. לחץ Start, הצבע על Settings, בחר את Control Panel, לחץ לחיצה כפולה על הסמל Add/Remove Programs, ולחץ על Add/Remove Windows Component.
2. גלול את הרשימה Components כלפי מטה, וסמן את הרשומה Networking Services.
3. לחץ על Details.
4. ברשימה Subcomponents of Networking Services סמן את הרשומה Dynamic Host Configuration Protocol (DHCP), לחץ OK, ולחץ Next.

   אם תתבקש, הקלד את הנתיב המלא לתיקיה בה מאוחסנים קבצי ההתקנה של Windows 2000, ולחץ Continue. הקבצים הנדרשים יועתקו לכונן הדיסק הקשיח שלך.
5. לחץ Finish כדי לסגור את Windows Components Wizard.

הערה מומלץ מאוד להגדיר את שרת ה-DHCP לשימוש בכתובת IP קבועה (סטטית). שרת DHCP אינו יכול להיות לקוח DHCP, בשל כך חייבים להיות מוגדרים בו כתובת IP קבועה, כתובת Subnet Mask וכתובת Default Gateway.

Ipconfig

Ipconfig היא תוכנית שירות המופעלת משורת הפקודה ואשר מציגה את התצורה הנוכחית של מחסנית IP (IP Stack) המותקנת במחשב המרושת. היא יכולה להציג דוח תצורה מפורט עבור כל הממשקים, כולל Miniports של רשת מרחבית (WAN) מוגדרת, כגון אלה המשמשים לצורך חיבורי גישה מרחוק או לחיבורי VPN (**V**irtual **P**rivate **N**etwork). דוח לדוגמה מוצג בתרשים 10.4.

```
Command Prompt
Windows 2000 IP Configuration

        Host Name . . . . . . . . . . . . : vb6entsvr
        Primary DNS Suffix  . . . . . . . : trainingassociates.com
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : Yes
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : trainingassociates.com

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : trainingassociates.com
        Description . . . . . . . . . . . : 3Com EtherLink XL 10/100 PCI TX NIC
(3C905B-TX)
        Physical Address. . . . . . . . . : 00-10-4B-65-14-6C
        DHCP Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 209.125.198.226
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 209.125.198.1
        DNS Servers . . . . . . . . . . . : 24.1.240.33
                                            24.1.240.34
                                            209.125.198.2
        Primary WINS Server . . . . . . . : 209.125.198.90

C:\>_
```

תרשים 10.4 הדוח המופק על ידי הפקודה ipconfig /all

מתגים של הפקודה Ipconfig

הפקודה Ipconfig נועדה לשימוש ברשתות בהן פועל DHCP, והיא מאפשרת למשתמשים לקבוע איזה ערכי תצורה הוגדרו על ידי DHCP עבור TCP/IP. טבלה 10.2 מסבירה את המתגים (Switches) המשמשים עם הפקודה Ipconfig.

טבלה 10.2 מתגי הפקודה Ipconfig

מתג	השפעתו
/all	מפיק דוח תצורה מפורט של כל הממשקים.
/flushdns	מסיר את כל הרשומות ממטמון שמות DNS.
/registerdns	DND name להסדרת לקוחות.
/displaydns	מציג את תוכן המטמון של DNS Resolver.
/release <adapter>	משחרר את כתובת ה-IP של המתאם המצוין.
/renew <adapter>	מחדש את כתובת ה-IP של המתאם המצוין.
/showclassid <adapter>	מציג את כל מזהי המחלקות (Class IDs) של DNS, המורשים למתאם המצוין.
/setclassid <adapter> <ClassID to set>	משנה את המזהה מחלקת DHCP עבור המתאם המצוין.
/?	מציג את הנתונים המופיעים בטבלה זו.

הערה ניתן להפנות את הפלט לקובץ ואז להדביקו במסמך אחר.

➢ **כדי לוודא, לשחרר או לחדש חוזה חכירה על כתובת לקוח**

1. במחשב שהוא לקוח מאופשר-DHCP הפועל בסביבת Windows 2000 פתח חלון שורת פקודה.
2. היעזר בפקודת שורת הפקודה Ipconfig כדי לוודא, לשחרר או לחדש את החוזה של הלקוח בשרת ה-DHCP, בדרך הבאה:

   כדי לוודא את הגדרות TCP/IP ו-DHCP הנוכחיות, הקלד ipconfig /all.

   כדי לשחרר את חוזה לקוח ה-DHCP, הקלד ipconfig /release.

   כדי לחדש את חוזה לקוח ה-DHCP, הקלד ipconfig /renew.

בתוכנית השירות Ipconfig ניתן להשתמש גם בסביבת Windows NT. כדי לבצע את אותן משימות בלקוחות Windows 9x השתמש בתוכנית Winipcfg, תוכנית הגדרת IP של Windows. כדי להפעיל את התוכנית Winipcfg בלקוחות התומכים בה, הקלד winipcfg בחלון MS-DOS או בתיבת הטקסט Open של תיבת דו-שיח Run. כדי לבצע פעולת שחרור או חידוש בתוכנית Winipcfg לחץ על לחצן Release או Renew (בהתאמה).

סוכן הממסר של DHCP

סוכן ממסר (Relay Agent) הוא תוכנית זעירה המשמשת כממסר בין הודעות DHCP/BOOTP לבין לקוחות ושרתים ב-Subnets אחרות. רכיב DHCP Relay Agent המסופק עם נתב Windows 2000 הוא סוכן ממסר BOOTP אשר משמש כממסר הודעות DHCP בין לקוחות DHCP לבין שרתי DHCP ברשתות IP אחרות. עבור כל מקטע רשת IP המכיל לקוחות DHCP דרוש שרת DHCP, או מחשב המשמש כסוכן ממסר DHCP.

➢ **כדי להוסיף את סוכן DHCP**

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ולחץ על Routing and Remote Access.
2. ב- MMC Tree לחץ על Server name\IP Routing\General.
3. לחץ לחיצה ימנית על General, ולחץ על New Routing Protocol.
4. בתיבת דו-שיח Select Routing Protocol לחץ על DHCP Relay Agent, ולחץ OK.

סיכום שיעור

DHCP פותח כדי לפתור בעיות הגדרה על ידי ריכוז נתוני הגדרת IP עבור לקוחות מסוימים. DHCP משתמש בתהליך בן ארבעה שלבים כדי להגדיר לקוח. השלבים, לפי הסדר, הם: גילוי חכירה, הצעת חכירה, בקשת חכירה ואישור חכירה. בנוסף לווידוא תצורת IP, תוכל להיעזר בתוכנית השירות Ipconfig כדי לחדש אפשרויות, לבחון את משך הזמן שנשאר לתוקפה של תקופת החכירה וכדי לבטל חכירה.

שיעור 2: הגדרת DHCP

בשיעור זה תלמד כיצד להגדיר את DHCP בשרת מבוסס-Windows 2000.

לאחר שיעור זה, תוכל

- לזהות את היתרונות שבשימוש ב-DHCP ברשת.
- להגדיר שרת ולקוחות DHCP.

זמן לימוד משוער: 10 דקות

שימוש ב-DHCP ברשת

הגדרת שרתי DHCP ברשת תספק לך את היתרונות הבאים:

- ❖ מנהל המערכת יכול להקצות ולציין פרמטרים של TCP/IP אשר הם גלובליים או ייחודיים ל- Subnet, ואשר ישמשו בכל הרשת.
- ❖ מחשבי הלקוח אינם דורשים הגדרות TCP/IP ידניות.

  כאשר מחשב לקוח עובר ל-Subnet אחרת, משוחררת כתובת ה-IP הישנה שלו. הגדרות TCP/IP של המחשב מוגדרות מחדש באופן אוטומטי כאשר הוא מאותחל במיקומו החדש.
- ❖ רוב הנתבים מסוגלים להעביר בקשות הגדרה של DHCP ושל BOOTP, כך שלא נדרש שרת DHCP בכל רשת משנה ברשת.

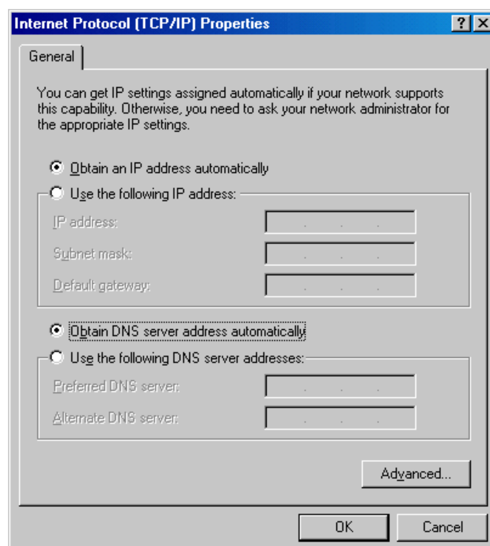
כיצד משתמשים הלקוחות בשרתי DHCP

מחשב הפועל בסביבת Windows 2000 הופך ללקוח DHCP אם בתיבת הדו-שיח של מאפייני TCP/IP שלו מסומנת התיבה Obtain an IP address, כפי שמוצג בתרשים 10.5.

כאשר מחשב לקוח מוגדר להשתמש ב-DHCP הוא מקבל הצעת חכירה ויכול לקבל מהשרת:

- ❖ שימוש זמני בכתובת IP הידועה ככתובת חוקית ברשת אליה הוא מצטרף.
- ❖ פרמטרים נוספים להגדרות TCP/IP אחרות בהן יוכל להיעזר, במבנה של נתונים אופציונליים.

בנוסף, אם מוגדר זיהוי התנגשויות, מנסה שרת DHCP לבצע PING לכל כתובת זמינה במרחב (Scope), לפני שהוא מציע אותה בהצעת חכירה ללקוח. פעולה זו מבטיחה שכל כתובת IP המוצעת ללקוח אינה נמצאת בשימושו של לקוח שאינו לקוח-DHCP, ואשר משתמש בהגדרות TCP/IP ידניות. מרחבי כתובות (Scopes) נדונים בשלב מתקדם יותר של שיעור זה.



תרשים 10.5 הגדרת הלקוח כך שישיג את כתובת ה-IP שלו משרת DHCP

כיצד מספקים שרתי DHCP נתונים אופציונליים

בנוסף לכתובת IP יכולים שרתי DHCP להיות מוגדרים, כך שיספקו נתונים אופציונליים כדי להגדיר את TCP/IP במלואו בלקוח. חלק מסוגי האפשרויות השכיחים ביותר של DHCP המוגדרים ומופצים על ידי שרת DHCP בעת חכירה כוללים :

- ❖ שערי ברירת מחדל (Default Gateways, Routers) המשמשים לחיבור בין מקטעי הרשת השונים.
- ❖ פרמטרי הגדרה אופציונליים נוספים המוקצים ללקוחות DHCP, כגון כתובת IP של שרתי DNS או שרתי WINS בהם יכול הלקוח להיעזר להסדרת שמות מארחים ברשת.

התקנה והגדרה של שרת DHCP

שירות DHCP Server חייב להיות פעיל כדי לתקשר עם לקוחות DHCP. לאחר ששרת DHCP הותקן והופעל יש להגדיר בו מספר אפשרויות. הצעדים הבאים הם צעדים כלליים להתקנה והגדרה של שרת DHCP :

- ❖ התקן את השירות Microsoft DHCP Server.
- ❖ אשר (Authorize) את שרת DHCP.
- ❖ לפני ששרת DHCP יוכל להחכיר כתובות IP ללקוחות DHCP, יש להגדיר בו מרחב (Scope) או מאגר (Pool) של כתובות IP חוקיות.
- ❖ ניתן להגדיר אפשרויות Global Scope או Client Scope עבור לקוחות DHCP מסוימים.
- ❖ ניתן להגדיר את שרת DHCP כך שתמיד יקצה את אותה כתובת IP לאותו לקוח DHCP.

אישור שרת DHCP

כאשר הם מוגדרים כהלכה ומאושרים לשימוש ברשת, שרתי DHCP מספקים שירות ניהולי יעיל. אבל, כאשר מופעל ברשת שרת DHCP שאינו מוגדר כהלכה או שלא אושר לשימוש ברשת הוא עלול לגרום לבעיות. למשל, אם מופעל שרת DHCP שלא אושר, הוא עשוי להתחיל ולהחכיר ללקוחות כתובות IP לא נכונות, או לשלוח אישורים שליליים (Negative Acknowledgments) ללקוחות DHCP המנסים לחדש את החכירה הנוכחית שלהם. כל אחת מההגדרות הללו עלולה לגרום לבעיות נוספות ללקוחות DHCP. לדוגמה, לקוחות שקיבלו חוזה חכירה משרת שלא אושר יכולים שלא לאתר כהלכה Domain Controllers, מה שימנע מהם לבצע כניסה תקינה לרשת.

כדי למנוע בעיות מסוג זה ב- Windows 2000, נערך לשרתים וידוא חוקיות ברשת לפני שהם יכולים לספק ללקוחות שירותים. דבר זה מונע את רוב הנזקים העלולים להיגרם כתוצאה מהפעלת שרתי DHCP שאינם מוגדרים כראוי, או שהם מוגדרים נכון, אך פועלים ברשת הלא נכונה.

כיצד מאשרים שרתי DHCP

שרתי DHCP הפועלים בסביבת Windows 2000 Server חייבים לעבור את תהליך האישור (Authorization). כדי שהתהליך Directory Authorization יפעל כהלכה נוצרת ההנחה, וכך גם צריך הדבר להיות, ששרת DHCP הראשון שהוצג בפני הרשת משתתף בשירותי Active Directory. דבר זה דורש שהשרת יהיה מותקן כ- Domain Controller או כ- Member Server (שרת חבר). כאשר אתה מתכנן או מיישם בפועל את שירותי Active Directory, חשוב שלא תבחר להתקין את שרת ה-DHCP הראשון שלך כ- Stand-Alone Server (שרת עצמאי). Windows 2000 Server מספק תמיכה באבטחה משולבת עבור רשתות המפעילות Active Directory. הדבר מונע את רוב הנזק האקראי הנגרם כתוצאה מהפעלת שרתי DHCP שאינם מוגדרים נכון, או ברשת הלא נכונה.

תהליך האישור למחשבי שרת DHCP ב- Active Directory תלוי בתפקידו של השרת ברשת שלך. ב- Windows 2000 (כמו גם בגרסאות הקודמות) קיימים שלושה תפקידים, או שלושה סוגי שרתים שניתן להגדיר:

1. **Domain Controller**. המחשב מאחסן ומתחזק עותק של מסד הנתונים של שירות Active Directory ומספק חשבון ניהול מאובטח למשתמשים ומחשבים שהם חברים ב-Domain.
2. **שרת חבר** (Member Server). המחשב אינו מתפקד כ- Domain Controller, אך מצטרף ל-Domain בו יש לו חשבון במסד הנתונים של שירות Active Directory.
3. **שרת עצמאי** (Stand-Alone Server). מחשב זה אינו מתפקד כ- Domain Controller או כ- Member Server ב-Domain. במקום זאת, מחשב השרת מוכר לרשת באמצעות שם קבוצת עבודה מסוים, אשר יכול להיות משותף עם מחשבים נוספים, אך הוא משמש רק למטרות עיון (Browsing) ואינו מספק גישה מאובטחת למשאבי domain משותפים.

אם אתה מיישם Active Directory, לפני שיוכלו לקבל אישור בשירות ה-Directory ולספק שירותי DHCP ללקוחות, כל המחשבים הפועלים כשרתי DHCP חייבים להיות Domain Controllers או Member Servers ב-Domain.

➢ כדי לאשר מחשב כשרת DHCP ב- Active Directory

1. התחבר לרשת באמצעות חשבון משתמש שיש לו הרשאות ניהול בארגון כולו, או באמצעות חשבון שהוסמך לאשר שרתי DHCP בארגון.

   ברוב המקרים, יהיה זה פשוט ביותר להתחבר לרשת מהמחשב אותו אתה מעוניין לאשר כשרת DHCP החדש. דבר זה מבטיח שהגדרות TCP/IP אחרות של המחשב המאושר הוגדרו כהלכה קודם לאישור. בדרך כלל, תוכל להשתמש בחשבון משתמש שהוא חבר בקבוצה Enterprise Administrators. החשבון בו אתה משתמש חייב לאפשר לך הרשאות Full Control באובייקט המכולה (Container Object) NetServices, מפני שהוא מאוחסן בשורשו של שרות Active Directory של הארגון.

2. אם יש צורך בכך, התקן את שירות DHCP במחשב זה.

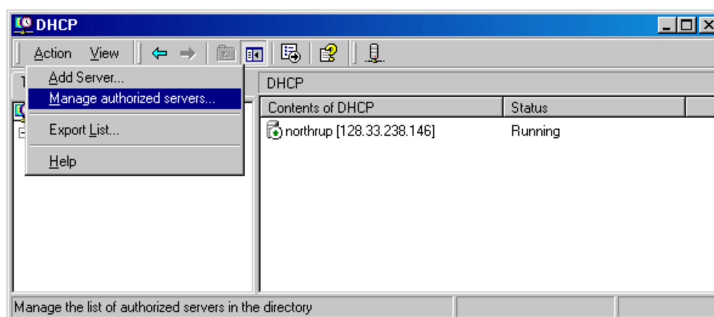
3. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ובחר DHCP.

4. פתח את תפריט Action ובחר את Manage authorized servers, כפי שמוצג בתרשים 10.6.

   מופיעה תיבת דו-שיח Manage Authorized Servers.

5. לחץ על Authorize.

6. כאשר תתבקש, הקלד את השם או כתובת ה-IP של שרת DHCP שאמור להיות מאושר, ולחץ OK.



תרשים 10.6 אישור שרת DHCP

הגנה בפני שרתי DHCP שאינם מאושרים

Active Directory משמש כיום לאחסון רשומות של שרתי DHCP מאושרים. כאשר "עולה" שרת DHCP, יכול כעת ה-Directory לשמש לצורך וידוא מצבו של שרת זה. אם שרת זה אינו מאושר, לא תוחזר תגובה כלשהי לבקשות DHCP. מנהל רשת בעל הרשאות הגישה המתאימות חייב להגיב. מנהל ה-domain יכול להקצות גישה לתיקיית DHCP בה שמורים נתוני התצורה, כדי לאפשר רק למורשים בכך להוסיף שרתי DHCP לרשימה המאושרת.

את רשימת השרתים המאושרים ניתן ליצור ב- Active Directory באמצעות יישום ה-Snap-In של DHCP. כאשר הוא "עולה" לראשונה מנסה שרת DHCP לברר אם הוא מופיע כחלק מה- Directory Domain. אם כן, הוא מנסה להתחבר ל-Directory, כדי לבדוק אם הוא מופיע ברשימת השרתים המאושרים. אם הוא מצליח, הוא שולח הודעת DHCPINFORM, כדי לברר אם פועלים שירותי Directory נוספים, ומוודא שהוא מאושר גם באחרים. אם הוא אינו מצליח להתחבר ל-Directory הוא מניח שהוא אינו מאושר, ואינו מגיב לבקשות מצד הלקוחות. בדומה, אם הוא כן מגיע ל-Directory, אך אינו מוצא את שמו ברשימת השרתים המאושרים, הוא אינו מגיב לבקשות מצידם של לקוחות. אם הוא מוצא את עצמו ברשימת המאושרים, הוא מתחיל לשרת את הלקוחות.

יצירת מרחב DHCP

לפני ששרת DHCP יוכל להחכיר כתובות ללקוחות DHCP, עליך ליצור מרחב (Scope). Scope הוא מאגר של כתובת IP חוקיות הזמינות לחכירה על ידי לקוחות DHCP. לאחר שהתקנת את שירות DHCP והוא פעיל, הצעד הבא יהיה יצירת המרחב. כאשר אתה יוצר מרחב DHCP, קח בחשבון את הנקודות הבאות:

- עליך ליצור מרחב אחד לפחות לכל שרת DHCP.
- עליך להשמיט מהמרחב את כתובת ה-IP הסטטיות שחלקת.
- תוכל ליצור מספר מרחבים בשרת DHCP, כדי לרכז את הניהול וכדי להקצות כתובות IP ייחודיות ל-Subnet. ניתן להקצות מרחב אחד בלבד לכל רשת משנה מסוימת.
- שרתי DHCP אינם משתפים נתוני מרחבים. כתוצאה מכך, כשאתה יוצר מרחבים במספר שרתי DHCP, עליך לוודא שלא תיווצר כפילות כתובות בין מרחבים, כדי למנוע כפילות מיעון IP של לקוחות.
- לפני שאתה יוצר מרחב, קבע את כתובת ההתחלה ואת כתובת הסיום שישמשו מרחב זה.

בהתאם לכתובת IP הפותחת ולכתובת IP המסיימת DHCP MMC מציעה Subnet Mask היעילה עבור מרבית הרשתות. אם ידוע לך שנדרשת Subnet Mask שונה עבור הרשת שלך, תוכל לשנות את הערכים כפי הנדרש.

כדי ליצור מרחב חדש

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ובחר DHCP.
2. ב- MMC Tree לחץ על שרת DHCP המבוקש.
3. פתח את תפריט Action, ובחר New Scope.
4. עקוב אחר ההוראות שבאשף New Scope Wizard.

כשתסיים ליצור את המרחב החדש ייתכן שתצטרך להשלים מספר משימות נוספות, כגון הפעלת המרחב לשימוש או הקצאת אפשרויות למרחב.

לאחר שנוספו מרחבים

לאחר שאתה מגדיר מרחב תוכל להמשיך ולהגדיר אותו על ידי ביצוע המשימות הבאות:

- **קבע טווחים מנועים (Exclusions) נוספים.** תוכל למנוע את חלוקתן של כתובות שאינן אמורות להיות מחולקות ללקוחות DHCP. עליך להשתמש במניעה (Exclusion) עבור כל ההתקנים שחייבים להיות מוגדרים באופן ידני. הטווחים המנועים צריכים לכלול את כל כתובות ה-IP אותן אתה מקצה באופן ידני לשרתי DHCP אחרים, ללקוחות שאינם לקוחות DHCP, לתחנות עבודה חסרות דיסקים (Diskless Workstation) או ללקוחות Routing and Remote Access או Point-to-Point (PPP).

- **קבע מאגרי כתובות שמורות (Reservations).** תוכל לבחור לשמור כמה כתובות IP, לשם החכרה קבועה למחשבים או התקנים מסוימים ברשת. עליך לבצע שמירה רק עבור התקנים שהם מאופשרי-DHCP (DHCP-Enabled) וכתובות אלו חייבות להיות שמורות למטרה מסוימת ברשת שלך (כגון שרתי הדפסה).

  אם אתה שומר כתובת IP עבור לקוח חדש, או כתובת שהיא אחרת מזו הנוכחית, עליך לוודא שהכתובת לא הוחכרה על ידי שרת ה-DHCP. שמירת כתובת IP מתוך מרחב אינה מחייבת באופן אוטומטי את הלקוח שכרגע משתמש באותה כתובת להפסיק את השימוש בה. אם הכתובת נמצאת בשימוש, צריך הלקוח המשתמש בה לשחרר אותה על ידי הפקת הודעת שחרור של DHCP. כדי לגרום לזה להתבצע במערכת Windows 2000 הקלד את הפקודה ipconfig /release בחלון שורת פקודה. שמירת כתובת בשרת DHCP גם אינה מחייבת שהלקוח החדש, שבעבורו נשמרה הכתובת, יעבור מייד להשתמש דווקא בה. גם במקרה זה צריך הלקוח קודם כל ליזום הודעת בקשה (DHCP Request). כדי לגרום לזה להתבצע במערכת Windows 2000 הקלד בחלון שורת פקודה את הפקודה ipconfig /renew.

- **התאם את תוקף החכירה.** תוכל לשנות את משך תוקף החכירה על ידי הקצאת חכירת כתובות IP. ברירת המחדל לאורך חייו של חוזה חכירה היא שמונה ימים. ברוב הרשתות המקומיות (LAN) ערך זה מספק, אך ניתן להגדילו אם רק לעיתים רחוקות עובר מחשב או משנה את מיקומו. ניתן אף להגדיר שאורך החיים של החכירה יהיה אין-סופי, אך יש להשתמש באפשרות זו בזהירות הראויה.

- **הגדר אפשרויות ומחלקות בהן יש להשתמש במרחב.** כדי לספק הגדרת תצורה מלאה ללקוחות יש להגדיר ולאפשר את אפשרויות DHCP עבור המרחב. לניהול מתקדם לא רציף של מרחב הלקוחות תוכל להוסיף או לאפשר מחלקות אפשרויות (Option Classes), המוגדרות על ידי משתמש או יצרן.

טבלה 10.3 מתארת חלק מהאפשרויות הזמינות בתיבת דו-שיח - Configure DHCP Options: Scope Properties, וכוללת את כל האפשרויות הנתמכות על ידי לקוחות DHCP של Microsoft.

טבלה 10.3 אפשרויות הגדרה של מרחב DHCP

אפשרות	תיאור
003 Router	מציינת את כתובת ה-IP של נתב, כגון כתובת שער ברירת המחדל. אם ללקוח מוגדר שער ברירת מחדל באופן מקומי, מקבלת הגדרה זו קדימות על הגדרת ה-DHCP.
006 DNS Servers	מציינת את כתובת IP של שרת DNS.
015 DNS Domain name	DNS name עבור הסדרת לקוחות.
044 WINS/NBNS servers	מציינת את כתובת ה-IP של שרת WINS הזמין עבור הלקוחות. אם מוגדרת בלקוח כתובת של שרת WINS באופן ידני, מקבלת הגדרה זו קדימות על הגדרת ה-DHCP.
046 WINS/NBNS node type	מציינת את סוג הסדרת השמות NetBIOS over TCP/IP בהן ישתמשו הלקוחות. האפשרויות הן: **1**= B-Node (Broadcast), **2**= P-Node (Peer-to-Peer), **4** = M-Node (Mixed) **ואילו 8** = H-Node (Hybrid).
047 NetBIOS Scope ID	מציינת את מזהה מרחב NetBIOS המקומי. NetBIOS over TCP/IP יתקשר רק עם מארחי NetBIOS אחרים המשתמשים באותו מרחב.

יישום מספר שרתי DHCP

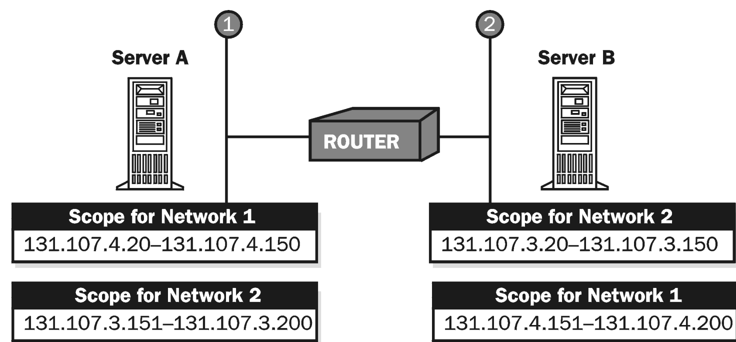
אם אגד הרשתות שלך דורש מספר שרתי DHCP, יש צורך ליצור מרחב ייחודי עבור כל רשת משנה. כדי להבטיח שהלקוח יכול לחכור כתובות IP במקרה של תקלה בשרת חשוב שיהיו מוגדרים מספר מרחבים עבור כל רשת משנה, הפזורים בין שרתי ה-DHCP באגד הרשתות. לדוגמה:

- לכל שרת DHCP צריך להיות מרחב המכיל כ- 75% ממספר כתובות ה-IP של רשת המשנה המקומית.
- לכל שרת DHCP צריך להיות מרחב עבור כל רשת משנה מרוחקת, המכיל כ- 25% מכתובות ה-IP הזמינות עבור אותה רשת משנה.

כאשר שרת ה-DHCP של הלקוח אינו זמין, עדיין יכול הלקוח לחכור כתובת משרת DHCP אחר ברשת משנה אחרת, בהנחה שהנתב שבין רשתות המשנה הוא סוכן ממסר של DHCP.

כפי שניתן לראות בתרשים 10.7, לשרת A יש מרחב (Scope) עבור רשת המשנה המקומית, כאשר הטווח (Range) שלו הוא בין 131.107.4.20 לבין 131.107.4.150, ואילו לשרת B יש מרחב בו טווח הכתובות הוא בין 131.107.3.20 לבין 131.107.3.150. כל שרת יכול להחכיר כתובות ללקוחות ברשת המשנה שלו.

בנוסף, לכל שרת יש מרחב המכיל טווח קטן של כתובות IP עבור רשת המשנה המרוחקת. לדוגמה, בשרת A יש מרחב עבור רשת משנה 2 ובו טווח הכתובות שבין 131.107.3.151 לבין 131.107.3.200 ואילו לשרת B יש מרחב כתובות עבור רשת משנה 1, בטווח הכתובות שבין 131.107.4.151 לבין 131.107.4.200. כאשר לקוח מרשת משנה 1 אינו מצליח להחכיר כתובת משרת A הוא ינסה לחכור אחת השייכת לרשת המשנה שלו משרת B, ולהיפך.



תרשים 10.7 מרחב וטווחי כתובות IP עבור שרת A ושרת B

סיכום שיעור

מרחב (Scope) הוא טווח (Range) של כתובות IP הזמינות לחכירה או להקצאה עבור לקוחות. כדי לאפשר ללקוחות DHCP להשיג כתובות IP חוקיות משרתי DHCP ניתן ליצור מספר מרחבים נפרדים עבור כל רשת משנה. כדי ליישם DHCP נדרשת תוכנה בצד הלקוח ובצד השרת. לכל שרת DHCP נדרש לפחות מרחב אחד.

שיעור 3:
שילוב DHCP עם Naming Services

שרת DHCP של Windows 2000 יכול לאפשר עדכונים דינמיים עם מרחב השמות של DNS עבור כל הלקוחות התומכים בעדכונים כגון אלה. אז, יכולים לקוחות מרחב (Scope Clients) להשתמש בפרוטוקול העדכון הדינמי של DNS כדי לעדכן את נתוני מיפויי שם-לכתובת שלהם (אשר מאוחסנים באזורים, Zones, בשרת DNS) כאשר מתרחשים שינויים לכתובות מוקצות-DNS שלהם. בשיעור זה תלמד כיצד לשלב את DHCP עם DNS.

לאחר שיעור זה, תוכל

- לשלב את DNS עם DHCP.
- לתאר כיצד פועל עדכון דינמי של DNS.
- לזהות כיצד מתנהלים עדכונים של לקוחות DHCP.

זמן לימוד משוער: 25 דקות

DNS ו- DHCP

למרות ש-DHCP מספק מנגנון בעל עוצמה להגדרת כתובות IP של לקוחותיו, עד לפני זמן קצר לא התריע DHCP בפני שירות DNS לעדכן את רשומות DNS בלקוח - ובמיוחד, עדכון שם הלקוח לכתובת IP ומיפוי כתובת IP-לשם, המנוהל על ידי DNS. אם לא קיימת דרך בה יכול DHCP לתקשר עם DNS, המידע המאוחסן ב-DNS עבור לקוחות DHCP עשוי להיות לא נכון. לדוגמה, לקוח יכול לקבל את כתובת ה-IP שלו משרת DHCP, אך רשומות ה-DNS לא ישקפו את כתובת ה-IP שהוקצתה, או את מיפוי הכתובת לשם המחשב (FQDN).

רישום לעדכוני DNS דינמיים

ב- Windows 2000, שרתי DHCP ולקוחותיהם יכולים להירשם ב-DNS, אם השרת תומך בעדכוני DNS דינמיים. שירות DNS של Windows 2000 תומך בעדכונים כאלה. שרת DHCP של Windows 2000 יכול לרשום בשרת DNS ולעדכן רשומות משאבים (RRs) מסוג מצביע (PTR) וכתובת (A) בשמם של לקוחות מאופשרי-DHCP, תוך שימוש בפרוטוקול העדכון הדינמי של DNS (DNS Dynamic Update Protocol). היכולת לרשום הן רשומות מסוג PTR והן רשומות מסוג A מאפשרת לשרת DHCP לשמש כחייץ (Proxy) עבור לקוחות Windows 95 ו- Windows NT, למטרת רישום DNS. שרתי DHCP יכולים להבחין בין Windows 2000 ולקוחות אחרים. קוד אופציה (Option Code) נוסף של DHCP (נקרא Option Code 81) מאפשר את החזרת ה-FQDN של לקוח לשרת DHCP. אם מיושם, שרת DHCP יכול לעדכן באופן דינמי את DNS כך שישנה רשומות משאבים (RRs) של מחשב מסוים בשרת DNS תוך שימוש בפרוטוקול העדכון של DNS. אופציית DHCP מאפשרת לשרת DHCP את אפשרויות הפעולה ההדדית הבאות לשם עיבוד נתוני DNS בשמם של לקוחות DHCP, הכוללים את Option Code 81 בהודעות בקשת DHCP הנשלחות על ידיהם לשרת:

- ❖ שרת DHCP תמיד רושם ב-DNS את לקוחות DHCP לחיפוש לפנים (Forward Lookup, רשומה סוג A) וחיפוש לאחור (Reverse Lookup, רשומה סוג PTR).

❖ שרת DHCP לעולם אינו רושם את נתוני המיפוי שם-לכתובת (רשומה מסוג A) של לקוחות DHCP.

❖ שרת DHCP רושם את לקוח DHCP הן לחיפוש לפנים (Forward Lookup, רשומה סוג A) והן לחיפוש לאחור (Reverse Lookup, רשומה סוג PTR), אבל רק כאשר הוא מתבקש לעשות זאת על ידי הלקוח.

DHCP ושירות DNS הסטטי אינם תואמים לשמירת הסינכרון של נתוני מיפוי שם-לכתובת. דבר זה עלול לגרום לבעיות בעת השימוש ב-DHCP וב-DNS יחד ברשת, אם אתה משתמש בשרתי DNS סטטיים מיושנים, אשר אינם מסוגלים לתקשר באופן דינמי כאשר מתרחש שינוי בתצורת לקוח DHCP.

➢ **כדי להימנע מכשלים בחיפוש DNS אחר לקוחות רשומי-DHCP, כאשר שירות DNS סטטי פעיל**

1. אם ברשת פועלים שרתי WINS, אפשר את חיפוש WINS עבור לקוחות DHCP המשתמשים ב-NetBIOS.
2. ללקוחות DHCP המשתמשים ב-DNS בלבד, ואינם תומכים ב-NetBIOS, הקצה שמירת כתובות IP עם אורך חיי חוזה חכירה אין-סופי.
3. בכל מקום בו הדבר אפשרי, שדרג או החלף שרתים מיושנים, מבוססי DNS-סטטי, בשרתי DNS התומכים בעדכונים. עדכונים דינמיים נתמכים על ידי DNS של Microsoft המצורף כחלק ממערכת ההפעלה Windows 2000.

המלצות נוספות

כאשר משתמשים ב-DNS יחד עם WINS יש לשקול את שילובי הפעולות הבאים:

❖ אם אחוז גדול של הלקוחות משתמשים ב-NetBIOS ואתה משתמש ב-DNS, שקול להשתמש בחיפוש (Lookup) של WINS בשרתי DNS שלך. אם חיפוש WINS פעיל בשרתי DNS של Microsoft, משמש WINS להסדרה הסופית של כל השמות שלא נמצאו באמצעות הסדרת DNS. החיפוש לפנים של WINS ורשומות WINS-R של החיפוש לאחור של WINS נתמכים רק על ידי DNS. אם אתה משתמש ברשת שלך בשרתים שאינם תומכים ב-DNS, היעזר ב- DNS Manager כדי להבטיח שרשומות WINS אלו אינן מופצות לשרתי DNS שאינם תומכים בחיפושי WINS (WINS Lookup).

❖ אם יש לך אחוז גבוה של מחשבי Windows 2000 ברשת, שקול ליצור סביבת DNS טהורה. הדבר מחייב תוכנית להגירת (Migration Plan) לקוחות WINS מיושנים לסביבת Windows 2000. נושאי תמיכה הקשורים לשירות שמות רשת מופשטים על ידי השימוש בשירות יחיד לאיתור ומיעון משאבים (כגון WINS או DNS) ברשת.

לקוחות DHCP של Windows ופרוטוקול העדכון הדינמי של DNS

ב- Windows 2000 Server, DHCP Server מספק שירות תמיכה של ברירת מחדל לרישום ועדכון נתונים עבור לקוחות DHCP מיושנים (Legacy) באזורי DNS. לקוחות מיושנים כוללים בדרך כלל מחשבי לקוח של TCP/IP, בגרסאות הקודמות ל- Windows 2000. השילוב של DNS/DHCP המסופק ב- Windows 2000 Server מאפשר ללקוח DHCP אשר אינו מסוגל לעדכן באופן דינמי רשומות משאבים (RRs) של DNS לעדכן מידע זה ישירות לאזורי החיפוש לפנים (Forward Lookup Zone) ולאחור (Reverse Lookup Zone) על ידי שרת ה-DHCP.

➤ כדי לאפשר עדכונים דינמיים עבור לקוחות DHCP אשר אינם תומכים בעדכוני DNS דינמיים

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ובחר DNS.
2. ב- MMC Tree לחץ על האזור (Zone) המבוקש.
3. פתח את תפריט Action, ובחר Properties.
4. בכרטיסיה DNS Properties סמן את Enable updates for DNS clients that do not Support dynamic update.
5. סמן את Only secure updates if your zone type is Active Directory-Integrated.

לקוחות DHCP הפועלים בסביבת Windows 2000 וגרסאות מוקדמות יותר של Windows מתקשרים ביניהם באופן שונה כאשר הם מבצעים את אינטראקציית DHCP/DNS (DNS/DHCP Interaction), שהוזכרה קודם לכן. הקטע הבא מסביר כיצד משתנה תהליך זה בהתאם למקרה.

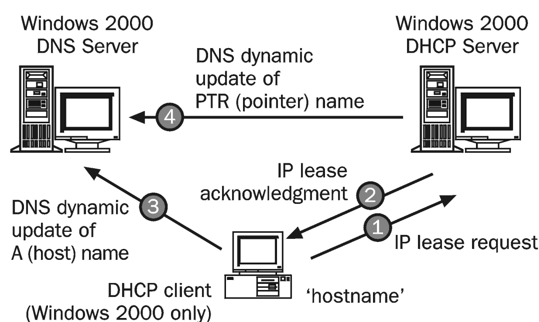
אינטראקציית DNS/DHCP Update עבור לקוחות DHCP של Windows 2000

לקוחות DHCP של Windows 2000 מתקשרים עם פרוטוקול העדכון הדינמי של DNS כך :

1. הלקוח יוזם הודעת בקשת DHCP (DHCPREQUEST) לשרת.
2. השרת משיב הודעת אישור DHCP (DHCPACK) ללקוח, בה מובטחת חכירת כתובת IP.
3. כברירת מחדל, שולח הלקוח בקשת עדכון DNS לשרת DNS עבור רשומת החיפוש לפנים של עצמו, רשומת משאב מארחת מסוג (A).

   לחילופין, יכול השרת לבצע עדכון זה בשרת ה-DNS בשמו של הלקוח, אם גם הלקוח וגם הגדרותיו משתנים בהתאם.
4. השרת שולח עדכונים לרשומת החיפוש לאחור של לקוח ה-DHCP (רשומת משאב מסוג PTR) תוך שימוש בתהליך המוגדר על ידי פרוטוקול העדכון הדינמי של DNS.

תהליך זה מתואר בתרשים 10.8.



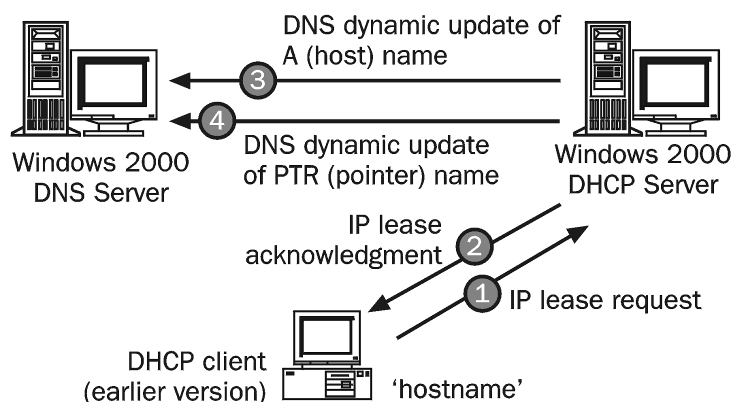
תרשים 10.8 אינטראקציה של לקוח DHCP עם פרוטוקול העדכון הדינמי של DNS

אינטראקצייה DNS/DHCP Update עבור לקוחות DHCP של גרסאות קודמות ל- Windows 2000

גרסאות קודמות של לקוחות DHCP אינן תומכות בתהליך העדכון הדינמי הישיר של DNS, ובשל כך אינן יכולות ליצור אינטראקציה ישירה עם שרת DNS. בדרך כלל, מטופל נושא העדכונים עבור לקוחות DHCP אלה כך :

1. הלקוח יוזם הודעת בקשת DHCP (DHCPREQUEST) לשרת.
2. השרת משיב הודעת אישור DHCP (DHCPACK) ללקוח, בה מובטחת חכירת כתובת IP.
3. השרת שולח עדכון לשרת DNS עבור רשומת החיפוש לפנים של הלקוח, שהיא רשומת משאב מארחת מסוג (A).
4. השרת שולח גם עדכונים לרשומת החיפוש לאחור של לקוח ה-DHCP, שהיא רשומת משאב מסוג PTR.

תהליך זה מתואר בתרשים 10.9.



תרשים 10.9 אינטראקציית DHCP/DNS עם לקוחות Windows מיושנים

סיכום שיעור

ב- Windows 2000 יכול שרת DHCP לאפשר עדכונים דינמיים במרחב השמות של DNS עבור כל אחד מלקוחותיו, התומך בעדכונים מסוג זה. כאשר מדובר בעדכונים דינמיים, יכול השרת העיקרי של אזור להיות מוגדר גם כך שיתמוך בעדכונים הייזומים על ידי מחשב או התקן אחר התומך בעדכונים דינמיים. לדוגמה, הוא יכול לקבל עדכונים מתחנת עבודה הרושמת רשומות משאבים מסוג A ומסוג PTR, או משרתי DHCP.

שיעור 4:
שימוש ב-DHCP עם Active Directory

DHCP של Microsoft מספק אינטגרציה עם שירות Active Directory ושירות DNS, ניטור מתקדם ודוחות סטטיסטיים עבור שרתי DHCP, אפשרויות מתואמות-יצרן ותמיכה במחלקות-משתמש, הקצאת כתובות Multicast ואיתור שרת DHCP מתחזה (Rogue).

לאחר שיעור זה, תוכל

- לתאר כיצד כתובת IP וניהול מיעון שמות מתבצע באמצעות אינטגרציית DHCP עם Active Directory.
- לתאר כיצד מאומתים שרתי DHCP.

זמן לימוד משוער: 15 דקות

אינטגרציית ניהול IP ב- Windows 2000

שירותי מיעון השמות והכתובות של Windows 2000 מציעים את הגמישות הדרושה להקלה בניהול רשתות עם מערכות מיעון שמות וכתובות אחרים. כפי שהיה הדבר ב- Windows NT Server גירסה 4.0, Windows 2000 Server מספקת שירותי DHCP, DNS ו-WINS כדי להמשיך לפשט את תהליך הקצאת והסדרת השמות. הדבר החדש שניתן למצוא ב-Windows 2000 Server הוא התמיכה ב-DNS דינמי, אינטגרציית DHCP ו-DNS ל-Active Directory ואת סוכן הממסר של DHCP.

שירותי הקצאת שמות וכתובות

ניהול כתובות IP ומיעון שמות פשוט יותר על ידי אינטגרציית Active Directory. לקוחות (Customers) יכולים לבחור להשתמש ב- Active Directory לצורך שכפול וסינכרון מיעון שמות DNS לכל אורך ורוחב הרשת הארגונית. דבר זה מפחית את הצורך לתחזק שירות שכפול ייעודי נפרד עבור DNS. השילוב של שירותי DHCP עם DNS דינמי עושה שימוש במידע הרשום ב-Directory, כדי לספק הקצאת כתובות ושירותי שמות. כאשר DHCP מקצה כתובות, DNS ו- Active Directory מעודכנים באופן דינמי. הדבר מאפשר למנהלי מערכת (Administrators) להקצות שוב כתובות לתחנות קצה, והסדרת השם מעודכנת באופן אוטומטי, כך שניתן לאתר אותן בקלות יתירה.

תמיכה בשרתים מיושנים

הפעולה המשולבת (Interoperability) עם שירותי DHCP ו-DNS מאפשרת שימור השקעה בשירותים קיימים. ללקוחות ניתנת האפשרות לבחור להשתמש במערכות מיושנות לניהול שמות וכתובות IP תוך שימוש ב-DHCP, סוכן הממסר של DHCP ו/או שירות DNS של Windows 2000 Server. העברת אזור (Zone Transfer) סטנדרטית ותמיכה בהפניות

מבטיחים שה-DNS של Windows 2000 Server יפעל במשולב עם שרתי DNS אחרים, לשם הסדרת שמות בארגון ובאינטרנט. דבר זה מאפשר ללקוחות להשתמש בשירותים המשולבים של Active Directory עבור הרשת שלהם, בעודם שומרים על שילוב פעילות האינטרנט ומערכות DNS ארגוניות אחרות. לדוגמה, חברה יכולה ליישם DNS ו-DHCP המשולבים בשירותי Active Directory עבור החלק העיקרי של הרשת, ועדיין לפעול במשולב עם שרתי DNS מיושנים. עם הזמן, תשתית ניהול ה-IP מבוססת-Active Directory יכולה להיות מורחבת בעוד שנשמרת הפעולה ההדדית עם שירותי DNS חיצוניים.

DHCP של Windows 2000 משולב גם באופן דינמי ב-DNS של Windows 2000, כתמיכה ב- Active Directory. גרסאות קודמות של DNS אינן מציעות תמיכה מסוג זה, ועליך לשקול עדכון גירסה (Upgrading) אם בכוונתך ליישם את Active Directory, או שאתה מעוניין להשתמש באיזון עומסים ברשת (Network Load Balancing).

תכונת הזיהוי של שרת DHCP מתחזה

שירות DHCP של Windows 2000 מציג תכונה המאפשרת לזהות שרת DHCP מתחזה (Rogue DHCP Server Detection). דבר זה מונע משרת DHCP מתחזה (כזה שאינו מורשה) מלהצטרף לרשת DHCP קיימת, בה מיושמים Windows 2000 ושירותי Active Directory. אובייקט שרת DHCP נוצר ב- Active Directory בו רשומות כתובות ה-IP של השרתים המורשים לספק שירותי DHCP לרשת. כאשר שרת DHCP מנסה להתחיל לשרת את הרשת מתבצעת שאילתה ל-Active Directory וכתובת ה-IP של מחשב זה מושווית לרשימת כתובת ה-IP של שרתי DHCP מורשים. אם נמצאה התאמה, מאושר מחשב השרת כשרת DHCP וניתנת לו האפשרות לסיים את תהליך האתחול שלו. אם לא נמצאה התאמה, מזוהה המחשב כמתחזה (Rogue) ושירות DHCP נסגר באופן אוטומטי.

סיכום שיעור

ניהול כתובות IP ומיעון שמות הופך לקל יותר באמצעות אינטגרציית Active Directory. כאשר DHCP מקצה כתובות, DNS ו-Active Directory מעודכנים באופן אוטומטי. פעולה משולבת עם שירותי DNS ו-DHCP אחרים מסייעת בשימור ההשקעה בשירותים קיימים, מפני שאתה יכול להשתמש במערכות ניהול מיעוני שמות וכתובות IP מיושנות עם שרתי DHCP של Windows 2000 Server. תהליך אימות של מחשב שרת DHCP ב-Active Directory תלוי בהיות השרת Domain Controller, Member Server או Stand-Alone Server. בנוסף, Active Directory משמש כעת לאחסון רשומות של שרתי DHCP מאושרים, כדי להגן בפני שרתי DHCP שאינם מורשים. את רשימת שרתי DHCP המורשים ניתן ליצור ב- Active Directory באמצעות יישום ה-Snap-In של DHCP.

שיעור 5: איתור וטיפול בתקלות DHCP

הבעיה השכיחה ביותר בלקוח DHCP היא כשל בקבלת כתובת IP, או נתוני הגדרה אחרים משרת DHCP בעת אתחול המערכת. הבעיות השכיחות ביותר בשרת DHCP הן חוסר האפשרות להפעיל את השרת ברשת בסביבת Windows 2000 או בסביבת Domain של Active Directory וכשלון מצד הלקוחות להשיג נתוני תצורה משרת פעיל. בשיעור זה תלמד כיצד לאתר ולטפל בתקלות בשרת DHCP ובלקוחות DHCP.

לאחר שיעור זה, תוכל

- לזהות ולפתור תקלות בלקוחות DHCP.
- לזהות ולפתור תקלות בשרת DHCP.

זמן לימוד משוער: 35 דקות

מניעת תקלות DHCP

תקלות DHCP רבות כוללות נתוני תצורה או הגדרה חסרים. כדי לסייע במניעת רוב התקלות השכיחות עליך לפעול כך:

- **השתמש בחוק 75/25 של תכנון איזון ביזור מרחב הכתובות, כאשר מיושמים מספר שרתי DHCP לשירות אותו מרחב.** השימוש ביותר מאשר שרת DHCP אחד באותה Subnet מספק Fault Tolerance גבוהה יותר לשם שירות לקוחות DHCP, המהווים חלק מה-Subnet. כאשר קיימים שני שרתי DHCP, אם אחד מהם הופך לבלתי זמין יכול השני לתפוס את מקומו ולהמשיך להחכיר כתובות IP חדשות, או לחדש כתובות קיימות.
- **בסביבת LAN, השתמש ב-SuperScopes עבור מספר מרובה של שרתי DHCP בכל Subnet.** Superscope (מרחב-על) מאפשר לשרת DHCP לספק חוזי חכירה ליותר מאשר מרחב אחד, ללקוחות ברשת פיסית אחת. כאשר הוא מופעל, משדר כל לקוח DHCP הודעת גילוי DHCP (DHCPDISCOVER) ל-Subnet שלו, בניסיון לאתר שרת DHCP. מכיון שלקוחות DHCP משתמשים ב-Broadcast בשלב האתחול שלהם, אינך יכול לצפות איזה שרת יגיב לשידור הגילוי של הלקוח (DHCPDISCOVER), במידה ומותקנים ופעילים יותר משרת DHCP אחד באותה Subnet.
- **בטל מרחבים רק במקרה של הסרה לצמיתות של מרחב מהשירות.** לאחר שהפעלת מרחב, אין לבטלו עד אשר פסק לחלוטין השימוש בו ובטווח הכתובות הנכלל בו ברשת שלך. לאחר שביטלת מרחב, שרת DHCP זה כבר אינו מקבל את כתובות מרחב זה ככתובות חוקיות.
- **השתמש בזיהוי-התנגשויות בצד השרת בשרתי DHCP רק כאשר הדבר נחוץ.** ניתן להשתמש בזיהוי-התנגשויות בשרתי DHCP או בלקוחות, כדי לקבוע אם נעשה שימוש בכתובת IP כלשהי ברשת, וזאת לפני החכרת או השימוש בה.

- **שמירות (Reservations) צריכות להתבצע בכל שרתי DHCP אשר ייתכן שיישרתו את הלקוח עבורו מתבצעת השמירה.** תוכל להשתמש בשמירה עבור לקוח (Client Reservation) כדי להבטיח שלקוח DHCP מסוים יקבל תמיד את אותה כתובת IP כאשר הוא מאותחל. אם יש לך יותר מאשר שרת DHCP אחד הנגיש על ידי לקוח שמור, הוסף את השמירה בכל אחד משרתי ה-DHCP האחרים שלך.

- **לשיפור ביצועי השרת, זכור ש-DHCP הוא שירות המכביד על הדיסק. רצוי לרכוש חומרה לה מאפייני ביצועים הטובים ביותר האפשריים.** DHCP גורם לפעילות תכופה ומתמשכת בכונני הדיסק הקשיח של השרתים. כדי לספק את מיטב הביצועים לרשת, בעת רכישת החומרה עבור מחשב השרת שלך שקול שימוש בפתרונות אחסון כגון RAID 0 או RAID 5.

- **אפשר רישום יומן ביקורת (Audit Logging) לשם איתור וטיפול בתקלות.** כברירת מחדל, שירות DHCP מאפשר רישום יומן ביקורת עבור אירועים הקשורים בשירות. ב- Windows 2000 Server, רישום יומן שגיאות מספק כלי ניטור שירות לאורך זמן אשר מאפשר שימוש בטוח ומוגבל במשאבי כונן הדיסק הקשיח בשרת.

- **שלב את DHCP עם שירותים נוספים, כגון WINS או DNS.** ניתן להשתמש הן ב-WINS והן ב-DNS לשם רישום דינמי של מיפוי שם-לכתובת (Dynamic Name-to-Address Mapping) ברשת שלך. כדי לספק שירותי הסדרת שמות עליך לתכנן את שיתוף הפעולה בין DHCP לשירותים אלה. רוב מנהלי המערכות המיישמים DHCP מתכננים גם אסטרטגיה ליישום DNS ו-WINS.

- **השתמש במספר שרתי DHCP המתאים לספר לקוחות מאופשרי-DHCP הקיימים ברשת שלך.** ברשתות LAN קטנות (כגון Subnet יחידה שאינה משתמשת בנתבים) יכול שרת DHCP יחיד לשרת את כל הלקוחות מאופשרי-DHCP (DHCP-Enabled). ברשתות מנותבות מספר השרתים הנדרש תלוי במספר גורמים, כגון מספר לקוחות מאופשרי-DHCP, מהירות התעבורה בין קישורי הרשת, מחלקת כתובות ה-IP של הרשת (IP Address Class) ובין אם שירות DHCP משמש לשירות כל הרשת הארגונית או רק רשתות פיסיות נבחרות.

איתור וטיפול תקלות בלקוח DHCP

רוב התקלות המשויכות ל-DHCP מתחילות כשגיאות בהגדרת IP בלקוח, כך שמן הראוי להתחיל בנקודה זו. לאחר שווידאת שמקורה של תקלה המשויכת ל-DHCP אינה בלקוח, בחן את יומן אירועי המערכת ואת יומני ביקורת שרת ה-DHCP ונסה למצוא רמזים אפשריים. כאשר שירות DHCP אינו אותחל בדרך, יסבירו יומנים אלה את המקור לכשל בשירות או להפסקת פעולתו. מעבר לכך, תוכל להיעזר בתוכנית השירות Ipconfig משורת הפקודה כדי לקבל מידע אודות הפרמטרים המוגדרים ל-TCP/IP במחשב זה או במחשב מרוחק ברשת.

הקטע הבא מתאר תסמינים שכיחים לתקלות DHCP בלקוח. כאשר הלקוח נכשל בקבלת הגדרות תצורה, תוכל להיעזר במידע זה כדי לזהות במהירות את מקור הבעיה.

הגדרה לא חוקית של כתובת IP

אם ללקוח DHCP לא מוגדרת כתובת IP, או שכתובת ה-IP המוגדרת בו היא מסדרת 168.254.x.x, זאת אומרת שהלקוח אינו יכול לתקשר עם שרת DHCP לקבלת חוזה לחכירת כתובת IP. תקלה זו נובעת בשל כשל חומרה ברשת שלך, או מפני ששרת DHCP אינו זמין. אם מתרחשת תקלה כגון זו, עליך לוודא שחיבור הרשת של מחשב הלקוח תקין ופעיל. ראשית, בדוק שהחומרה הקשורה לרשת במחשב הלקוח (כבלים וכרטיסי רשת) פועלים כראוי.

תקלות הגדרת תצורה אוטומטית ברשת הנוכחית

אם ללקוח DHCP יש כתובת IP המוגדרת באופן אוטומטי (Autoconfigured) אשר אינה נכונה לרשת הנוכחית שלו, לקוח DHCP של Windows 98 ושל Windows 2000 אינו יכול לאתר שרת DHCP והוא משתמש בתכונה APIPA כדי לקבל כתובת IP. ברשתות גדולות מסוימות, רצוי לבטל תכונה זו לשם ניהול הרשת. APIPA מחוללת כתובת IP במבנה 169.254.x.y (כאשר x.y הוא המזהה הייחודי של הרשת אותו מחולל הלקוח) וכתובת Subnet של 255.255.0.0. שים לב ש-Microsoft שמרה את טווח הכתובות 169.254.0.1 ועד 169.254.255.254 ומשתמשת בו לתמיכה בתכונה APIPA.

➢ **כדי לתקן כתובת IP המוגדרת באופן אוטומטי באופן לא תקין**

1. ראשית, השתמש בפקודה PING כדי לבחון את החיבוריות בין הלקוח לבין השרת. אחר כך, נסה לחדש באופן ידני את חוזה החכירה של הלקוח. בהתאם לדרישות הרשת שלך, ייתכן שיימצא הצורך לבטל את התכונה APIPA בלקוח.

2. אם חומרת הלקוח עושה רושם תקין, בדוק ששרת ה-DHCP זמין ברשת. את הבדיקה ניתן לבצע על ידי ביצוע PING ממחשב אחר, אך אחד כזה שנמצא באותה רשת בה נמצא לקוח ה-DHCP בו התגלתה התקלה. מעבר לכך, אתה יכול לנסות לשחרר ולחדש את חכירת הכתובת בלקוח, ולבחון את הגדרות TCP/IP במיעון אוטומטי.

פרטי הגדרה חסרים

אם ללקוח DHCP חסרים פרטי הגדרה הוא עלול להפסיד חלק מאפשרויות DHCP בחוזה החכירה שלו, בין אם מפני ששרת ה-DHCP אינו מוגדר להפיץ הגדרות אלו ובין אם מפני שהלקוח אינו תומך באפשרויות המופצות על ידי השרת. אם קורה כדבר הזה בלקוחות DHCP של Microsoft, ודא שההגדרות השכיחות ביותר בשימוש והנתמכות על ידי מירב הלקוחות הוגדרו בשיוכי האפשרויות בין אם של השרת, המרחב (Scope), הלקוח או רמת המחלקה (Class Level). בחן את הגדרת אפשרויות DHCP.

לפעמים, משויכת ללקוח כל ערכת האפשרויות וההגדרות כהלכה, אבל הגדרות השרת שלו אינן פועלות כשורה. אם בשרת ה-DHCP מוגדרת אפשרות הנתב הלא נכונה (Option Code 3) עבור ה- Default Gateway של לקוחות מבוססי Windows 98 או קודמות לה, תוכל:

1. לשנות את רשימת כתובות ה-IP עבור אפשרות הנתב (Default Gateway) בשרת ומרחב DHCP המתאימים.

2. לקבוע את הערך הנכון בכרטיסיה Scope Options שבתיבת דו-שיח Scope Properties.

במקרים נדירים, ייתכן שתצטרך להגדיר את הלקוח כך שישתמש ברשימת שרתים השונה מזו המופיעה עבור לקוחות אחרים של אותו מרחב. במצבים כגון אלה, תוכל להוסיף שמירה (Reservation) ולהגדיר את רשימת הנתבים האפשריים עבור הלקוח שבעבורו בוצעה השמירה.

לקוחות Windows NT או Windows 2000 אינם משתמשים בכתובות שגויות, מפני שהם תומכים בתכונה Dead Gateway Detection (איתור שער "מת"). תכונה זו של פרוטוקול TCP/IP של Windows 2000 משנה את ה- Default Gateway ל- Default Gateway הבא ברשימת ה- Default Gateways, כאשר מספר מסוים של חיבורים מעבירים תשדורות חוזרות של מקטעים.

שרתי DHCP אינם מספקים כתובות IP

אם לקוחות DHCP אינם מצליחים לקבל כתובות IP מהשרת, אחד מהמצבים הבאים יכול לגרום לבעיה זו:

- ***כתובת ה-IP של שרת ה-DHCP שונתה, וכעת לקוחות DHCP אינם מסוגלים לקבל כתובות.*** שרת DHCP יכול לשרת רק בקשות למרחב לו יש מזהה רשת (Network ID) זהה למזהה הרשת של כתובת ה-IP. ודא שכתובת ה-IP של שרת ה-DHCP קיימת באותו טווח כתובות רשת של המרחב אותו הוא משרת. לדוגמה, שרת שכתובת ה-IP שלו היא חלק מהרשת 192.168.0.0 אינו יכול להקצות כתובות מהמרחב 10.0.0.0, אלא אם נעשה שימוש במרחבי-על (Superscopes).
- ***לקוחות DHCP ממוקמים מעבר לנתב מרשת המשנה בה קיים שרת ה-DHCP, ואינם מצליחים לקבל הקצאת כתובת מהשרת.*** שרת DHCP יכול לספק כתובות IP למחשבי לקוח במספר רשתות משנה מרוחקות, רק במידה והנתב המפריד בין אותן רשתות משנה יכול לשמש גם כסוכן ממסר DHCP. השלמת הצעדים הבאים יכולה לסייע לתיקון התקלה:

1. הגדר ברשת המשנה הלקוחה (Client Subnet, זאת אומרת באותו מקטע של הרשת הפיסית) סוכן BOOTP/DHCP. את הסוכן תוכל למקם בנתב עצמו או במחשב מבוסס Windows 2000 Server בו פועל רכיב שירות DHCP Relay.
2. בשרת ה-DHCP, הגדר מרחב התואם לכתובת הרשת מצידו השני של הנתב, היכן שממוקמים הלקוחות המושפעים מהבעיה.
3. במרחב זה, ודא שמסכת רשת המשנה תואמת לרשת המשנה המרוחקת.
4. אל תכלול מרחב זה (זה של רשת המשנה המרוחקת) במרחבי-על (Superscopes) המוגדרים לשימוש באותו מקטע או Subnet מקומית, הפועלים במקום בו פועל שרת ה-DHCP.

- **מספר שרתי DHCP קיימים באותה רשת מקומית (LAN).** ודא שאינך מגדיר מספר שרתי DHCP באותה רשת מקומית, אשר קיימים בהם מרחבים חופפים. ייתכן שתצטרך לשלול את האפשרות שאחד משרתי ה-DHCP הוא שרת SBS (**S**mall **B**usiness **S**erver). במקורו, שירות DHCP הפועל בסביבת SBS פוסק באופן אוטומטי מלפעול כאשר הוא מזהה שרת DHCP אחר ברשת המקומית.

איתור וטיפול בתקלות בשרת DHCP

כאשר שרת נכשל בהספקת חוזי חכירה ללקוחותיו, מתגלה כשל זה ברוב המקרים על ידי הלקוחות באחת מהדרכים הבאות:

1. ייתכן שללקוח תוגדר כתובת IP שאינה מסופקת על ידי השרת.
2. השרת שולח ללקוח הודעת תגובה שלילית, והלקוח מציג הודעת שגיאה או חלון מוקפץ המציין ששרת DHCP לא אותר.
3. השרת מקצה ללקוח כתובת, אבל נראה כאילו ללקוח יש בעיות אחרות המבוססות על הגדרות תצורת הרשת, כגון חוסר יכולת להירשם ולהסדיר שמות NetBIOS או DNS או להגיע למחשבים הנמצאים מעבר לרשת המשנה שלו.

פעולת האיתור והטיפול הראשונה שעליך לבצע היא לוודא ששירותי DHCP אכן פעילים. ניתן לבצע זאת על ידי פתיחת DHCP MMC וצפייה במצב (Status) השירות, או על ידי סקירת החלק Services שברשומת Services And Applications מחלון Computer Manager. אם השירות הנדרש אינו מופעל, הפעל אותו. במקרים נדירים, שרת DHCP אינו יכול להיות מופעל, או שעלולה להתרחש הודעת עצירה. אם שרת ה-DHCP נעצר, השלם את ההליך הבא כדי לאתחל אותו:

➢ **כדי להפעיל מחדש שרת DHCP שנעצר**

1. הפעל את Windows 2000 Server והיכנס למערכת באמצעות חשבון מנהל (Administrator).
2. פתח חלון Command Prompt (שורת פקודה), הקלד את הפקודה net start dhcpserver, והקש Enter.

הערה היעזר ב- Event Viewer מקבוצת Administrative Tools כדי לנסות ולאתר מקורות אפשריים לבעיות בשירותי DHCP.

שירות DHCP Relay Agent מותקן, אך אינו פועל

שירות DHCP Relay Agent מופעל באותו מחשב בו פועל שירות DHCP. מכיון ששני השירותים מאזינים ומגיבים להודעות BOOTP ו-DHCP הנשלחות ליציאות (Port) 67 ו- 68, אף לא אחד מהשירותים פועל באופן אמין אם שניהם מותקנים באותו מחשב. לפתירת הבעיה, התקן את רכיבי שירות DHCP ואת רכיבי שירות DHCP Relay Agent בשני מחשבים נפרדים.

DHCP MMC מדווח על תפוגת חוזי חכירה באופן שגוי

כאשר DHCP MMC מציג את שעת תפוגת חכירה של לקוחות שמורים במרחב, מצביע הדבר על אחד מהדברים הבאים:

❖ אם משך זמן החכירה של המרחב מוגדר כאין-סופי (Infinite), יוצג גם משך זמן החכירה של הלקוח כלא-סופי.

❖ אם משך זמן החכירה של המרחב מוגדר למשך זמן מסוים (Finite, למשל שמונה ימים), יוצג כך גם משך זמן החכירה של הלקוח.

תנאי החכירה של לקוח DHCP שמור נקבעים על ידי חוזה החכירה ששויך לשמירה (Reservation). כדי ליצור לקוחות שמורים עם משך זמן חכירה אין-סופי, צור מרחב לו זמן חכירה אין-סופי והוסף את השמירות למרחב זה.

שרת DHCP משתמש ב-Broadcast כדי להגיב על כל הודעות הלקוחות

שרת DHCP משתמש ב-Broadcast כדי להגיב לכל הודעות בקשת התצורה מהלקוחות, ללא קשר לאופן בו הציב כל לקוח DHCP את סיבית דגלון השידור שלו. לקוחות DHCP יכולים לקבוע את דגלון השידור כאשר הם שולחים הודעת DHCPDISCOVER, כדי לציין לשרת ה-DHCP שיש להשתמש בשידור לכתובת השידור המוגבל (Limited Local Broadcast Address שהיא 255.255.255.255) כאשר משיבים ללקוח את תגובת DHCPOFFER.

לידיעתך דגלון השידור, Broadcast Flag, הוא הסיבית הראשונה בשדה Flags בן 16 הסיביות שבכותרת הודעת DHCP.

כברירת מחדל, שרת DHCP של Windows NT Server 3.51 וגרסאות קודמות לו, התעלמו מדגלון השידור בהודעות DHCPDISCOVER, ושידרו רק תגובות DHCPOFFER. התנהגות זו מיושמת בשרת כדי למנוע בעיות העלולות להתרחש כתוצאה מכך שלקוחות אינם מצליחים לקבל או לעבד תגובה Unicast, לפני שייושמו בהם הגדרות TCP/IP.

מאז גירסה 4.0 של Windows NT Server ואילך, שירות DHCP עדיין מנסה לשלוח את כל תגובות DHCP כשידורי IP לכתובת השידור המוגבל, אלא אם התמיכה ב-Unicast מאופשרת, על ידי קביעת ערך רשומת רישום המערכת IgnoreBroadcastFlag ל- 1. רשומה זו נמצאת תחת HKEY_LOCAL_MACHINE\System\CurrentControl\Services\DHCPServer \Parameters\IgnoreBroadcastFlag. כאשר ערך רשומה זו הוא 1, לא מתייחסים לדגלון ה-Broadcast בהודעת הבקשה מהלקוח, וכל תגובות DHCPOFFER משודרות מהשרת ב-Broadcast. כאשר ערך הרשומה מוגדר ל- 0 (אפס) התנהגות תשדורת השרת (אם לשדר ב-Broadcast או לא) נקבעת על ידי הגדרת סיבית דגלון השידור שבבקשת DHCPDISCOVER של הלקוח. אם דגלון זה מוגדר בבקשה, משדר השרת את תגובתו לכתובת השידור המוגבל המקומית. אם דגלון זה אינו מוגדר בבקשה, השרת משדר את תגובתו ב-Unicast ישירות ללקוח.

שרת DHCP נכשל בהפקת חכירת כתובת עבור מרחב חדש

לשרת DHCP הוסף מרחב (Scope) חדש במטרה למספר מחדש את הרשת הקיימת. אבל, לקוחות DHCP אינם משיגים חוזי חכירה מהמרחב החדש. מצב זה שכיח במיוחד כאשר אתה מנסה למספר מחדש רשת IP קיימת. לדוגמה, ייתכן שהשגת מחלקה רשומה של כתובות IP עבור הרשת שלך, או ששינית את המחלקה כדי לארח מספר רב יותר של מחשבים או רשתות. במצבים כגון אלה תרצה שהלקוחות ישיגו את החכירה שלהם מהמרחב החדש, במקום להשתמש במרחב הישן. לאחר שכל הלקוחות קיבלו חוזי חכירה פעילים מהמרחב החדש, אתה מעוניין להסיר את המרחב הישן.

כאשר מרחבי-על אינם בשימוש או שאינם זמינים, יכול להיות רק מרחב DHCP אחד פעיל ברשת בכל רגע נתון. אם הוגדר והופעל יותר ממרחב אחד בשרת DHCP, ישמש רק מרחב אחד להספקת חוזי חכירה ללקוחות. המרחב הפעיל (Active Scope) אשר יקצה את החכירה ללקוחות, נקבע על פי טווח הכתובות המכיל את כתובת ה-IP הראשונה המאוגדת

(Bind) לחומרת מתאם הרשת של שרת ה-DHCP. כאשר כתובות IP משניות נוספות מוגדרות בשרת, תוך שימוש בכרטיסיה Advanced TCP/IP Properties, אין לכתובות אלו השפעה על שרת ה-DHCP לשם קביעת המרחב הנבחר או המגיב לבקשות הגדרת תצורה מלקוחות DHCP ברשת זו. בעיה מסוג זה ניתן לפתור באחת מהדרכים הבאות:

- הגדר את שרת ה-DHCP לשימוש במרחב-על (SuperScope) הכולל את המרחב החדש ואת המרחב הישן.
- שנה את כתובת ה-IP העיקרית (זו המוקצית בכרטיסיה TCP/IP Properties) של כרטיס מתאם הרשת בשרת ה-DHCP לכתובת IP, שהיא חלק מאותה הרשת כמו המרחב החדש.

במקרה של שרתי Windows NT גירסה 3.51 לא קיימת תמיכה במרחבי-על. במקרה כגון זה, ראשית עליך לשנות את כתובת ה-IP המוגדרת לכרטיס מתאם הרשת של שרת ה-DHCP לאחת הקיימת במרחב החדש. אם נמצא הצורך בכך, תוכל עדיין לשמר את הכתובת הישנה שהוגדרה לשרת זה ככתובת IP פעילה למחשב השרת, על ידי העברתה לרשימת כתובות ה-IP המנוהלת בכרטיסיה Advanced TCP/IP Properties.

ניטור ביצועי השרת

מכיון ששרתי DHCP הם בעלי חשיבות עליונה ברוב סביבות העבודה, פעולת ניטור ביצועי השרתים עשויה לסייע באיתור וטיפול בתקלות, במקרים בהם חלה הדרדרות בביצועי השרת. במקרה של שרת Windows 2000, שירות DHCP כולל ערכה של מוני ביצועים המאפשרים ניטור של סוגי פעילויות שונים של השרת. כברירת מחדל, מונים אלה זמינים לאחר התקנת שירות DHCP. כדי לגשת למונים אלה, עליך לפתוח את System Monitor (מנטר הרשת שהיה ידוע בעבר בשם Performance Monitor, מנטר הביצועים). מוני שרת DHCP מסוגלים לנטר:

- כל סוגי הודעות DHCP הנשלחות על ידי שירות DHCP.
- משך זמן ממוצע לעיבוד שמנצל שרת ה-DHCP עבור כל מנת הודעה נשלחת או מתקבלת.
- מספר מנות ההודעה שהושמטו (Dropped) בשל עיכובים פנימיים במחשב שרת ה-DHCP.

העברת מסד הנתונים של שרת DHCP

ייתכן שיימצא הצורך להעביר את מסד נתוני DHCP למחשב אחר. כדי לבצע פעולה זו השתמש בהליך הבא:

➢ כדי להעביר את מסד הנתונים של DHCP

1. עצור את שירות DHCP במחשב הנוכחי.
2. העתק את התיקיה System32\Dhcp\ למחשב החדש שהוגדר כשרת DHCP.

ודא שהתיקיה החדשה נוצרת בדיוק באותו מקום בו היתה התיקיה לפני העברתה (אותם אות כונן ונתיב תיקיה). אם עליך להעביר את הקבצים לתיקיה שונה, העתק את הקובץ DHCP.MDB, אך אל תעתיק את הקבצים בעלי הסיומות log או chk.

3. הפעל את שירות DHCP במחשב השרת החדש. באופן אוטומטי מתחיל השירות להשתמש בקבצי mdb ו-log שהועתקו מהמחשב הישן.

כשאתה בוחן את DHCP Manager המרחב עדיין קיים, מפני שרישום המערכת מחזיק את המידע אודות טווח הכתובות של המרחב, כולל מפת סיביות של כתובות הנמצאות בשימוש.

➢ כדי להשלים את מסד הנתונים של DHCP

1. בחלון DHCP manager פתח את תפריט Scope, ובחר Active Leases.
2. בתיבת דו-שיח Active Leases לחץ על Reconcile.

למרות שאין צורך בכך, תוכל לחייב לקוחות DHCP לחדש את חוזי החכירה שלהם, כדי לגרום לעדכון שרת ה-DHCP בהקדם האפשרי. כדי לעשות זאת, הקלד בשורת הפקודה את הפקודה ipconfig/renew.

סיכום שיעור

התקלה האופיינית ביותר בלקוח DHCP היא כשל בקבלת כתובת IP או פרמטרי הגדרה אחרים משרת ה-DHCP בעת תהליך האתחול. התקלה האופיינית ביותר בשרת DHCP היא חוסר האפשרות להפעיל את השרת ברשת הפועלת בסביבת Windows 2000 או בסביבת Domain של Active Directory. רוב תקלות ה-DHCP מתחילות בתקלה בהגדרת IP בלקוח, כך שמן הראוי להתחיל את תהליך איתור וטיפול בתקלות בנקודה זו.

שאלות סיכום

השאלות הבאות נועדו לחזק את הנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות על שאלה, עיין בשיעור המתאים ונסה את השאלה שנית. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואחר כך בעברית.

Answering the following questions will reinforce key information presented in this chapter. If you are unable to answer a question, review the appropriate lesson and then try the question again. Answers to the questions can be found in Appendix A, "Questions and Answers."

1. What is DHCP?
2. Describe the integration of DHCP with DNS.
3. What is a DHCP client?
4. What is IP autoconfiguration in Windows 2000?
5. Why is it important to plan an implementation of DHCP for a network?
6. What tool do you use to manage DHCP servers in Windows 2000?
7. What is the symptom of most DHCP-related problems?

1. מה זה DHCP?
2. תאר את האינטגרציה שבין DHCP לבין DNS.
3. מהו לקוח DHCP?
4. מהי הגדרה אוטומטית של IP (IP Autoconfiguration) בסביבת Windows 2000?
5. מדוע חשוב לתכנן לפני שמיישמים את DHCP ברשת?
6. באיזה כלי תשתמש כדי לנהל שרתי DHCP בסביבת Windows 2000?
7. מהו התסמין הראשון המצביע על תקלה הקשורה ל-DHCP?

פרק 11

מתן אפשרות גישה מרחוק ללקוחות

אודות פרק זה

בפרק זה תלמד כיצד ליישם את שירותי הגישה מרחוק, במטרה להעניק ללקוחות יכולת גישה למשאבי רשת ממיקומים מרוחקים. כמו כן, תלמד ליישם **רשתות פרטיות וירטואליות** (VPNs) מאובטחות.

לפני שתתחיל

להשלמת השיעורים בפרק זה נדרש:

- שני מחשבים ובכל אחד מהם מותקן ופועל שרת Windows 2000, בעלי חיבוריות לרשת תקשורת מקומית (LAN).

שיעור 1: הכרת RAS

תכונת הגישה מרחוק (Remote Access) של Windows 2000 Server מאפשרת גישה אל רשתות הארגון לעובדים מרוחקים או ניידים המחוברים בחיוג, כאילו היו מחוברים ישירות אליהן. שירות גישה מרחוק (**R**emote **A**ccess **S**ervice ,RAS) כולל גם שירותי VPN כך שהמשתמשים יכולים לקבל גישה לרשתות הארגון דרך האינטרנט.

לאחר שיעור זה, תוכל

- להסביר את תכונות שירות הגישה מרחוק.
- להתקין שירות גישה מרחוק.
- לתאר את ההבדלים בין שירות גישה מרחוק לבין שליטה מרחוק.
- להסביר את ההשפעה של שדרוג על Routing and Remote Access.

זמן לימוד משוער: 25 דקות

סקירת Remote Access Service

RAS, הגישה מרחוק של שרת Windows 2000, אשר מהווה חלק משירות RAAS (**R**outing and **R**emote **A**ccess **S**ervice) המשולב במערכת ההפעלה, מחברת עובדים מרוחקים או ניידים לרשתות הארגון. משתמשים מרוחקים יכולים לעבוד כאילו מחשביהם היו מחוברים פיסית לרשת הארגונית. משתמשים (או לקוחות ברשת) מפעילים תוכנת גישה מרחוק, כדי ליזום את תהליך ההתחברות לשרת הגישה מרחוק. שרת הגישה מרחוק, בעצמו מחשב מבוסס Windows 2000 Server בו RAAS מאופשר, מאמת (Authenticate) משתמשים ומשרת Sessions עד לסיומם. כל השירותים הזמינים באופן רגיל למשתמש המחובר ל-LAN (כולל שיתוף קבצים ומדפסות, גישה לרשת האינטרנט, ושירות ההודעות) מאופשרים באמצעות חיבור הגישה מרחוק.

לקוחות גישה מרחוק עושים שימוש בכלים סטנדרטים לצורך גישה למשאבי הרשת. לדוגמה, במחשב מבוסס Windows 2000 לקוחות יכולים להיעזר ב- Windows Explorer כדי למפות כוננים ברשת ולהתחבר למדפסות. מדובר בהתחברויות עמידות, ולכן המשתמשים לא צריכים להתחבר מחדש אל משאבי הרשת במשך ה- Remote Session. כיון שגישה מרחוק תומכת בצורה מלאה באותיות הכוננים ובשמות UNC (**U**niversal **N**aming **C**onvention), רוב היישומים המסחריים והמותאמים יכולים לעבוד ללא שינויים. שרת גישה מרחוק המבוסס Windows 2000 מספק שני סוגים שונים של חיבוריות גישה מרחוק:

- **רישות בחיוג.** רישות בחיוג (Dial-up Networking) מתקיים כאשר לקוח גישה מרחוק יוזם התחברות ארעית בחיוג אל יציאה פיסית של שרת גישה מרחוק באמצעות ספק שירותי תקשורת כגון קו טלפון אנלוגי, קו ISDN, או X.25. הדוגמה הטובה ביותר של רישות בחיוג היא זו של לקוח אשר מחייג את מספר הטלפון של אחת היציאות (Ports) של שרת גישה מרחוק.

רישות בחיוג באמצעות קו טלפון אנלוגי או קו ISDN הוא חיבור פיסי ישיר לקוח הרישות בחיוג (Dial-Up Client) לבין שרת הרישות בחיוג (Dial-Up Server). אפשר להצפין נתונים הנשלחים מעל חיבור כזה, אך הדבר לא נדרש לצורך יצירתו.

❖ **רישות פרטי וירטואלי.** VPN (**V**irtual **P**rivate **N**etworking) היא היצירה של קישור מאובטח מנקודה-לנקודה דרך רשת פרטית או ציבורית, כגון האינטרנט. לקוח VPN משתמש בפרוטוקולים מיוחדים מבוססי TCP/IP המכונים פרוטוקולי תיעול (Tunneling Protocols) במטרה ליזום קריאה אל יציאה (Port) בשרת VPN. הדוגמה הממשית ביותר של VPN היא של משתמש בחיוג המתחבר דרך האינטרנט לשרת ברשת הארגון. שרת הגישה מרחוק עונה לקריאה הווירטואלית, מאמת את זהות המתקשר, ומעביר את הנתונים בין לקוח ה-VPN לבין הרשת הארגונית.

בניגוד לרישות בחיוג, VPN הוא קישור לוגי (יותר מאשר חיבור פיסי) בין לקוח ה-VPN והשרת. כדי להבטיח פרטיות, יש להצפין את הנתונים הנשלחים מעל החיבור. בדרך כלל משתמשים בחיבורי VPN דרך האינטרנט כדי להפחית את עלויות החיבור.

תכונות Routing and Remote Access

ערכת התכונות Routing and Remote Access של Windows מספקת תרגום כתובות רשת (NAT, (**N**etwork **A**ddress **T**ranslation, L2TP (**L**ayer **Two** **T**unneling **P**rotocol), IAS (**I**nternet **A**uthentication **S**ervice) ו-RAP (**R**emote **A**ccess **P**olicies). פרק זה מסכם את המידע אודות מסנני חיוג-על-פי-דרישה (Demand-Dial Filters), שעות חיוג החוצה (Dial-Out, בהן תישלל הגישה בחיוג-על-פי-דרישה), מאפייני משתמש בחיוג פנימה, שימוש גישה מרחוק בשמות שרתים ו-DCHP, BAP (**B**andwith **A**llocation **P**rotocol) וניטור גישה מרחוק.

Router Discovery

ל-Windows 2000 יש תכונה חדשה המכונה גילוי נתב (Router Discovery), אשר מתוארת ב- RFC 1256. תכונת גילוי הנתב מספקת שיטה משופרת להגדרה וגילוי של שערי ברירת מחדל (Default Gateways). כאשר משתמשים ב-DHCP או בהגדרה ידנית של שער ברירת מחדל, לא קיימת דרך להתאמה לשינויים ברשת. באמצעות השימוש בגילוי נתב, לקוחות מגלים נתבים באופן דינמי ויכולים לעבור לנתבי גיבוי אם אירעה תקלה ברשת, או אם נדרש שינוי מנהלתי בה. תכונת גילוי הנתב מורכבת משני סוגי מנות (Packets):

1. **Router Solicitations.** כאשר יש צורך להגדיר שער ברירת מחדל למחשב מארח, התומך ב- RFC 1256, המארח שולח שידול נתב (Router Solicitation) באמצעות הודעת פרוטוקול ICMP (**I**nternet **C**ontrol **M**essage **P**rotocol). שידול הנתב יכול להישלח לכתובת 224.0.0.2, שהיא כתובת Multicast לכל נתבי ה-IP, או לכתובת Broadcast מוגבל, שהיא 255.255.255.255. בפועל, מארחים שולחים הודעות שידול נתב אל המען להפקת שידור IP לרבים (IP multicast address). נתבים ברשת של המארח אשר תומכים ב- RFC 1256 מגיבים באופן מיידי באמצעות פרסום נתב (Router Advertisement), והמארח בוחר בנתב בעל רמת העדיפות הגבוהה ביותר בתור שער ברירת המחדל שלו.
2. **Router Advertisements.** פירסומי נתב הן הודעות מפורשות למארחים ברשת על כך שהנתב עדיין זמין. נתב מוציא מודעת נתב מחזורית באמצעות הודעת ICMP. מודעת הנתב יכולה להישלח לכתובת השידור הרחב המקומית (Local IP Broadcast Address) המשדרת לכל המארחים, או לכתובת לשידור מוגבל. בדומה לשידורי נתבים, מודעות הנתבים נשלחות למעשה לכתובת ה-Multicast.

הערה Windows 2000 תומכת בגילוי נתבים הן כמארח והן כנתב.

(NAT) Network Address Translator

NAT הוא תקן המוגדר ב- RFC 1631. NAT הוא נתב המתרגם כתובות IP של אינטראנט או של רשת תקשורת מקומית (LAN) לכתובות אינטרנט חוקיות. NAT מאפשר לרשת פרטית עם כתובות פרטיות (Private Addresses) קישוריות לאינטרנט דרך כתובת IP ציבורית יחידה. מערכת ההפעלה Windows 2000 Server כוללת יישום NAT במתכונת מלאה, הנקרא Connection Sharing, ובנוסף גם גירסה נטולת הגדרות בשם Shared Access.

Multicast Routing

Windows 2000 Server מיישמת צורה מוגבלת של ניתוב שידור לרבים (Multicast Routing) תוך שימוש ב-Multicast Proxy. Multicast Proxy מאפשר הרחבת התמיכה ב-Multicast מעבר לזו של נתב Multicast אמיתי. השימוש המיטבי ב- Multicast Proxy הוא למתן אפשרות Broadcast למשתמשי גישה מרחוק, או לרשת LAN יחידה המחוברת לאינטרנט. בממשק אחד או יותר פועלת Windows 2000 כמו נתב Multicast, המתקשר עם לקוחות מקומיים באשר לצרכיהם ב-Multicast. בממשק בעל גישה ישירה לנתב multicast אמיתי, פועלת Windows 2000 כלקוח Multicast, המעביר תעבורת שידור IP לרבים (Multicast Traffic) לטובת הלקוחות המקומיים.

Layer Two Tunneling Protocol

L2TP (**L**ayer **2** **T**unneling **P**rotocol - פרוטוקול תיעול של שכבת קישור הנתונים) יכול להיחשב כגירסה מתקדמת של PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol). הוא פועל באופן מאוד דומה ל-PPTP, אך כיום הוא תוצר של פיתוח משותף עם חברת Cisco. L2TP הוא שילוב של פרוטוקול L2F (**L**ayer **2** **F**orwarding) על פי טכנולוגיה של Cisco, ושל פרוטוקול PPTP (על פי טכנולוגיות מיסודן של Microsoft, Ascend, 3Com, U.S. Robotics ו- ECI-Telematics). בעת כתיבת שורות אלו L2TP עדיין מוגדר כטיוטה ל-RFC, אך עד מהרה יהפוך לתקן בענף. L2TP הוא פרוטוקול של שכבה 2 (Data-Link Layer) לפי מודל OSI (**O**pen **S**ystems **I**nterconnection) לארכיטקטורת רשת תקשורת. זהו פרוטוקול המשמש ליצירת VPNs.

Internet Authentication Service

שירות אימות האינטרנט (IAS, **I**nternet **A**uthentication **S**ervice) הוא שרת RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) המספק שירותי אימות מרחוק למשתמש בחיוג פנימה לרשת. RADIUS הוא פרוטוקול רשת המאפשר אימות, אישור וניהול חשבון מרחוק של משתמשים המתקשרים לשרת גישה לרשת (NAS, **N**etwork **A**ccess **S**erver). שרת גישה לרשת כגון Routing and Remote Access יכול להיות שרת RADIUS או לקוח RADIUS.

הערה Microsoft שיחררה גירסה מוגבלת של RADIUS server ב- Option pack של Windows NT 4.0. גירסה מלאה של RADIUS server (IAS) זמינה כעת ב- Windows 2000.

Remote Access Policies

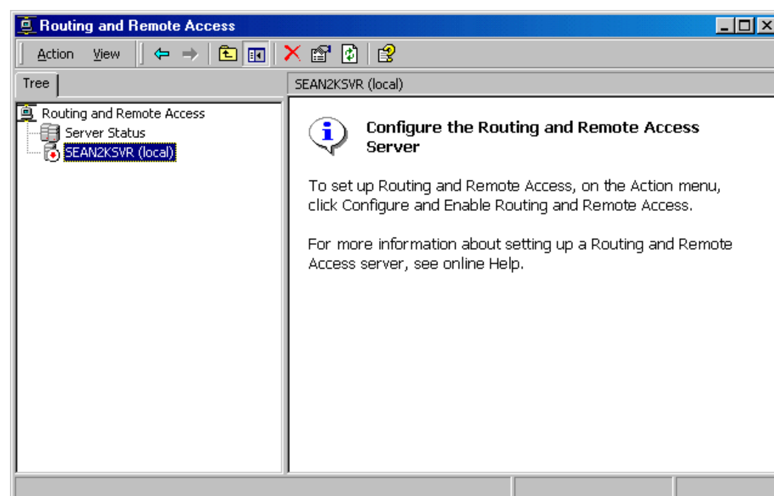
בגרסת Windows NT 3.5 ומאוחרות יותר, הוענקה גישה מרחוק המבוססת על אופציה פשוטה Grant Dial-In Permission To User, אשר ב- User Manager או בתוכנית השירות Remote Access Admin. אפשרויות להתקשרות חוזרת (Call Back) הוענקו גם הן על בסיס המשתמש-היחיד.

ב- Windows 2000 התחברויות גישה מרחוק מוענקות בהתבסס על מאפייני החיוג של חשבון המשתמש ועל ערכות מדיניות גישה מרחוק (RAPs, **R**emote **A**ccess **P**olicies). RAPs הן ערכות של תנאים ופרמטרים של חיבור, אשר מאפשרות למנהלי הרשת גמישות גדולה יותר בהענקת הרשאות לגישה מרחוק ואפשור השימוש ברשת. דוגמאות אחדות לתנאי ההתחברות כוללות את השעה ביום, קבוצה וסוג החיבור (VPN או חיוג). דוגמאות אחדות של פרמטרים בחיבור עשויות להיות דרישות אימות והצפנה, שימוש ב- Multilink ואורך ה-Session. דוגמה אחת לתועלת שבשליטה נוספת זו היא הדרישה להצפנה חזקה בהתחברויות VPN, או לעומת זאת, אי-הרשאה של הצפנה כלשהי בחיבורי מודם, היכן שאינה חיונית.

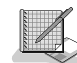
RAPs מאוחסנים במאגר המקומי והם משותפים ל- Routing and Remote Access ול-IAS של Windows 2000. מדיניות RAP מוגדרת באמצעות Internet Authentication Service Manager או באמצעות Routing and Remote Access Manager.

אפשור Routing and Remote Access

כעת, לאחר שהבנת את נושא הניתוב וגישה מרחוק, תיגש לאפשר את השירות. לפני שתאפשר את השירות ייראה ה- Routing and Remote Access Manager כמו זה שבתרשים 11.1.



תרשים 11.1 ה- Routing and Remote Access Manager לפני התקנה.



תרגול: התקנת Routing and Remote Access Server

בתרגול זה תתקין שרת Routing and Remote Access תוך שימוש ב- Routing and Remote Access Manager.

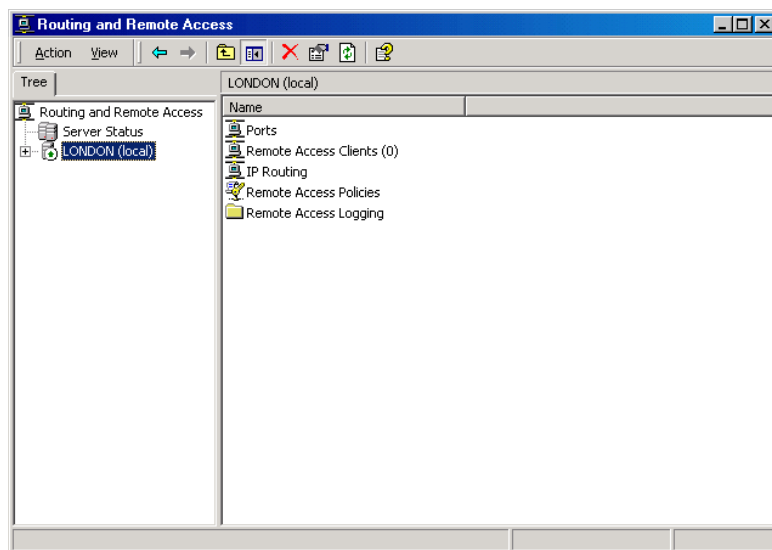


לפני שתמשיך בשיעור, הפעל את קובץ ההדגמה Ch11.exe הנמצא בתיקיה Media שבתקליטור המצורף לספר זה. הקובץ יספק סקירה אודות התקנת ה- Routing and Remote Access server.

➢ כדי להתקין את Routing and Remote Access Server

1. פתח את Routing and Remote Access Manager.
2. לחץ לחיצה ימנית על שם המחשב שלך, ומתפריט הקיצור בחר באפשרות Configure and Enable Routing and Remote Access.
3. בחלון Routing and Remote Access Server Setup Wizard לחץ Next.
4. בחלון Common Configuration בחר Remote Access Server, ולחץ Next.
5. בחלון Remote Clients Protocol, ודא ש-TCP/IP נמצא ברשימה Protocols. אם כן, ודא שהאפשרות Yes, All The Required Protocols Are On This List אכן נבחרה, ולחץ Next.
6. בחלון IP Address Assignment, ודא שהאפשרות From A Specified Range Of Addresses אכן נבחרה, ואז לחץ Next.
7. בחלון Address Range Assignment לחץ New. ליד Starting Address הקלד 10.0.0.10 (עבור- computer 1) ו- 10.0.0.20 (עבור- computer 2). מתחת ל- End Of IP Address הקלד 10.0.0.19 (עבור- computer 1) ו- 10.0.0.29 (עבור- computer 2). מתחת ל- Number Of Addresses, ודא שמצוין המספר 10. לחץ OK כדי לסגור את חלון Edit Address Range. לחץ Next.
8. בחלון Managing Multiple Remote Access Servers ודא שהאפשרות No, I Don’t Want To Set This Server Up To Use RADIUS Now נבחרה, ואז לחץ Next.
9. לחץ Finish.
10. אשר בלחיצת OK כל הודעת אזהרה שתופיע על המסך.

מראה Routing and Remote Access Manager יהיה דומה לזה שבתרשים 11.2.



תרשים 11.2 Routing and Remote Access Manager לאחר התקנה.

➢ כדי להעניק הרשאה לחיוג פנימה עבור חשבון המנהל

1. פתח את Directory Management (אם ב-domain), או את Computer Management Systems Tools, Local Computer Management (אם בקבוצת עבודה).
2. פתח את User Properties for Administrator, ובכרטיסיה Dial-In בחר באפשרות Allow Access.

גישה מרחוק לעומת שליטה מרחוק

ההבדלים בין פתרונות של גישה מרחוק ושל שליטה מרחוק הם הבאים:

- שרת הגישה מרחוק הוא נתב רב-פרוטוקולי מבוסס תוכנה. הפתרונות של גישה מרחוק פועלות על ידי שיתוף מסך, מקלדת ועכבר באמצעות הקישור המרוחק. בגישה מרחוק, היישומים מופעלים במחשב לקוח המרוחק.
- בפתרון של שליטה מרחוק, המשתמשים משתפים מעבד (CPU) אחד או רבים בשרת. בשליטה מרחוק, היישומים מופעלים בשרת. המעבד בשרת הגישה מרחוק, לעומת זאת, נועד לקיים את התקשורת בין לקוחות גישה מרחוק לבין משאבי הרשת, ולא להפעלת יישומים.

התוצאה של שדרוג ל- Windows 2000 על התכונה Routing and Remote Access

השדרוג מ- Remote Access Service/Routing and Remote Access Service של Windows NT 4.0 ל- Windows 2000 מלווה בבעיה קטנה. מערכת ההפעלה Windows NT גירסה 4.0 מאפשרת שימוש ב- LocalSystem account (חשבון של מערכת מקומית). כאשר שירות כלשהו מתחבר כ-LocalSystem הוא נכנס עם הרשאת התחברות **ריקה** (NULL credentials), ומשמעותה היא ששירות זה אינו מספק שם משתמש או סיסמה.

Active Directory בהגדרות ברירת המחדל שלו, לא מתיר ביצוע שאילתות על מאפייני אובייקטים ב-Sessions היזומים עם הרשאת התחברות NULL, ולכן בסביבה מעורבת נדרש תכנון כדי להרשות לשרתי Windows NT 4.0 RAS/RRAS לאחזר מ- Active Directory מאפייניהם של משתמשים בחיוג. שרתי RAS/RRAS זקוקים לגישה זו כדי לקבוע אם הוענקו למשתמש הרשאות חיוג, ואם הוגדרו מאפיינים נוספים כלשהם לחיוג פנימה, כגון מספרי טלפון להתקשרות חזרה (Call Back).

הערה השימוש בהרשאת התחברות מאופסת (NULL) מונע מהחשבון אפשרות גישה למשאבי הרשת הנשענת על אימות של Windows **NT L**AN **M**anager) NTLM) - אלא אם כן המחשב המרוחק מאפשר במפורש התחברויות בהרשאת NULL.

שיקולים לשדרוג Remote Access Server

כדי ששרת Windows NT 4.0 Remote Access Service/Routing ושירות Remote Access יוכל לאחזר מאפייני משתמש מ- Active Directory, עליך למלא אחד מהתנאים הבאים:

- יש לך Domain במצב מעורב (Mixed Mode) ושרת RAS/RRAS מבוסס Windows NT 4.0 שלך הוא גם Backup Domain Controller. במקרה זה, לשרת RAS/RRAS יש גישה למסד נתוני מנהל חשבונות האבטחה המקומי (Local SAM, Local Security Accounts Manager).
- יש לך Domain במצב מעורב ושרת RAS/RRAS של Windows NT 4.0 מתחבר למחשב Windows NT 4.0 BDC כדי לקבוע את מאפייני המשתמש בחיוג. זה גם יאפשר גישה למסד נתוני SAM המקומי.
- ה-Domain הוא במצב מעורב (Mixed Mode) או במצב טהור (Native Mode) והאבטחה של Active Directory שוחררה, כדי לאפשר להרשאות הטבעיות למשתמש Everyone לקרוא מאפיין כלשהו של אובייקט משתמש כלשהו. הדבר מוגדר באמצעות אשף ההתקנה של Active Directory (DCPROMO.EXE) על ידי בחירת אפשרות Permission Compatible With Pre-Windows 2000 Server.

הערה אפשר שההצלחה בחיבוריות תושג רק לסירוגין, אלא אם כן האבטחה של Active Directory שוחררה או ששרת RAS/RRAS הותקן ב-BDC. אפילו אם ה-Domain פועל במצב מעורב, לא ניתן להגדיר את שרת RAS/RRAS כדי שיתחבר ל-BDC של Windows NT גירסה 4.0 רק למטרת אימות. אם DC של Windows 2000 יאמת את המשתמש, ייכשל נסיון ההתחברות בחיוג.

בחירת האפשרות Permission Compatible With Pre-Windows 2000 Servers ממקמת את הקבוצה Everyone בקבוצה המקומית של גישה התואמת גרסאות קודמות ל-Windows 2000 (Pre-Windows 2000 Compatible Access Local Group). אפשר לשוב ולחזק את ההרשאות באמצעות המחיקה של הקבוצה Everyone מרשימת המשתייכים לקבוצה הרשומה מעלה, לאחר שכל שרתי הגישה מרחוק ישודרגו ל- Windows 2000.

הערה רצוי לעשות שימוש בעקיפה באמצעות הקבוצה Everyone רק לאחר ההבנה של השפעתה על האבטחה של Active Directory. אם זה סותר את דרישות האבטחה, מומלץ לשדרג את שרת Windows NT 4.0 RAS/RRAS ל- Windows 2000 ולהפוך אותו לחבר (Member) ב-domain טהור או מעורב של Windows 2000. צעד זה ימנע מתן לא עקבי של גישה למחייגים, כאשר ה-domain נמצא במצב מעורב.

אם רוצים לשחרר אבטחה כדי להרשות לשרתי Windows NT 4.0 RAS/RRAS לתפקד לאחר הפעלת אשף ההתקנה של Active Directory, אפשר להוסיף את הקבוצה Everyone לקבוצה Pre-Windows 2000 Compatible Access Group באמצעות הקלדת הפקודה
net localgroup "Pre-Windows 2000 Compatible Access" Everyone /add.

סיכום שיעור

שיעור זה סיפק סיכום בסיסי של תכונות הגישה מרחוק. זה כולל את תכונת גילוי הנתב, תרגום כתובות רשת (NAT), ניתוב שידור לרבים, פרוטוקול תיעול של שכבת קישור הנתונים (L2TP), שירות אימות האינטרנט (IAS) וערכות מדיניות גישה מרחוק (RAPs). כמו כן, נסקרו ההתקנה וההגדרה של Routing and Remote Access.

שיעור 2: הגדרת Routing and Remote Access Server

לאחר ששרת ניתוב וגישה מרחוק הותקן, תוכל להגדיר אותו עבור התחברויות נכנסות, לנעול אותו בעזרת ה-RAPs (**R**emote **A**ccess **P**olicies), להוסיף פרופילים של גישה מרחוק למטרות אבטחה, ולבקר על הגישה באמצעות BAP (**B**andwidth **A**llocation **P**rotocol). בשיעור זה, תבדוק אפשרויות הגדרה אלו.

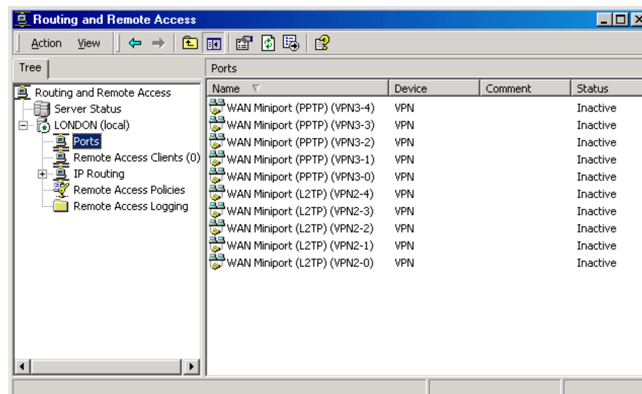
לאחר שיעור זה, תוכל

- להסביר איך להרשות התחברויות המועדות פנימה.
- לעצב מדיניות גישה מרחוק (RAP) חדשה.
- לתאר את דרך ההגדרה של פרופיל גישה מרחוק.
- לתאר את דרך ההגדרה של פרוטוקול הקצאת רוחב פס (BAP).

זמן לימוד משוער: 45 דקות

הרשאת התחברויות מועדות פנימה

כאשר Routing and Remote Access Manager מופעל בפעם הראשונה, יוצרת Windows 2000 באופן אוטומטי חמש יציאות (Ports) PPTP וחמש יציאות L2TP, כפי שמוצג בתרשים 11.3. כמות יציאות VPN הזמינות עבור שרת גישה מרחוק כלשהו אינה מוגבלת על ידי החומרה, וניתן להגדיר את מספרן. ניתן להגדיר יציאות VPN מהרשומה Ports ב-console tree של Routing and Remote Access.



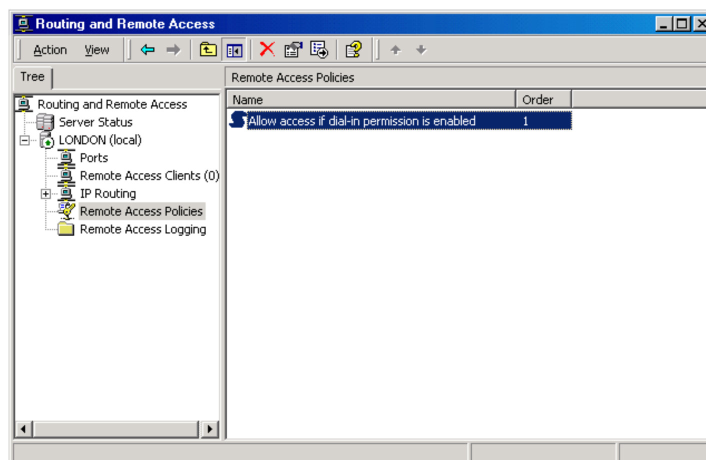
תרשים 11.3 יציאות Routing and Remote Access

תוכל גם להוסיף יציאה מקבילית (Parallel Port) על ידי הגדרת Ports. יציאות התקשורת הטוריות תוצגנה רק אחרי שיותקן מודם עבור מחשב הניתוב וגישה מרחוק. שני סוגי היציאות יכולים להיות מוגדרים עבור התחברויות נכנסות או יוצאות.

יצירת מדיניות גישה מרחוק (RAP)

RAPs (**R**emote **A**ccess **P**olicies) הם כינויים לערכות של תנאים, כפי שמודגם בתרשים 11.4, הבאים להגדיר למי יש גישה מרחוק לרשת, ומה יהיו מאפייני ההתחברות. התנאים להרשאה או שלילת התחברויות יכולים להתבסס על קריטריונים רבים ושונים, כגון היום והשעה, קבוצת החברות של האובייקט, סוג השירות וכך הלאה. מאפייני ההתחברות ניתנים להגדרה, למשל הגדרה שהתחברות ISDN יכולה להימשך עד 30 דקות ואשר לא תרשה מנות **HTTP** (**H**yper**t**ext **T**ransfer **P**rotocol).

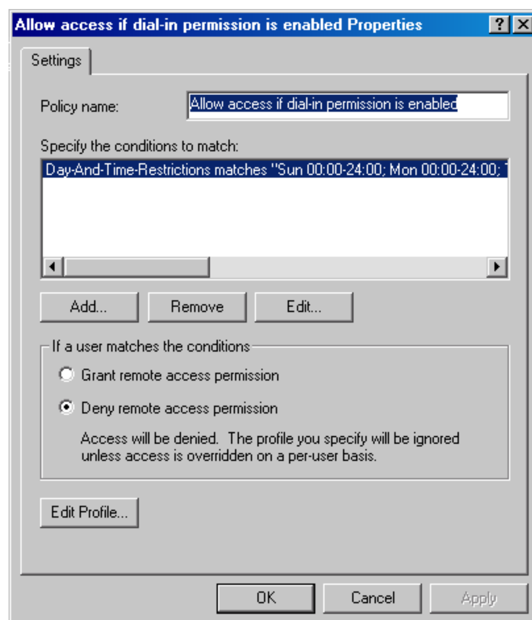
הערה ה-RAPs משותפות בין Routing and Remote Access ל-IAS. ניתן להגדיר אותן מכל אחד מהכלים האלה.



תרשים 11.4 Routing and Remote Access Policies

אפשר ליצור RAPs, למחוק אותן, לשנות שמן ולארגן אותן מחדש מתוך כלי הניהול של IAS או מתוך Routing and Remote Access Manager. שים לב שלא קיימת אפשרות Save, כך שלא ניתן לשמור עותק לדיסקט. יש משמעות לסדר בין ערכות המדיניות השונות, כיון שהערכה המתאימה הראשונה תשמש להרשאה או לשלילת ההתחברות.

הערה RAPs אינן מאוחסנות ב- Active Directory: הן מאוחסנות מקומית בקובץ IAS.MDB. חייבים ליצור את הערכות באופן ידני בכל שרת. Remote Access Policies מופעלות על משתמשים ב-domain ב-Mixed mode, אפילו אם ניתן להציב את הרשאת החיוג של המשתמש רק ל- Allow Access או Deny Access, כפי שמוצג בתרשים 11.5 (ניהול גישה באמצעות מדיניות גישה מרחוק אינו זמין ב- Mixed-Mode Domain Controllers. גם אם הרשאת המשתמש היא Allow Access, המשתמש עדיין צריך למלא את תנאי ערכת המדיניות לפני שיורשה להתחבר.



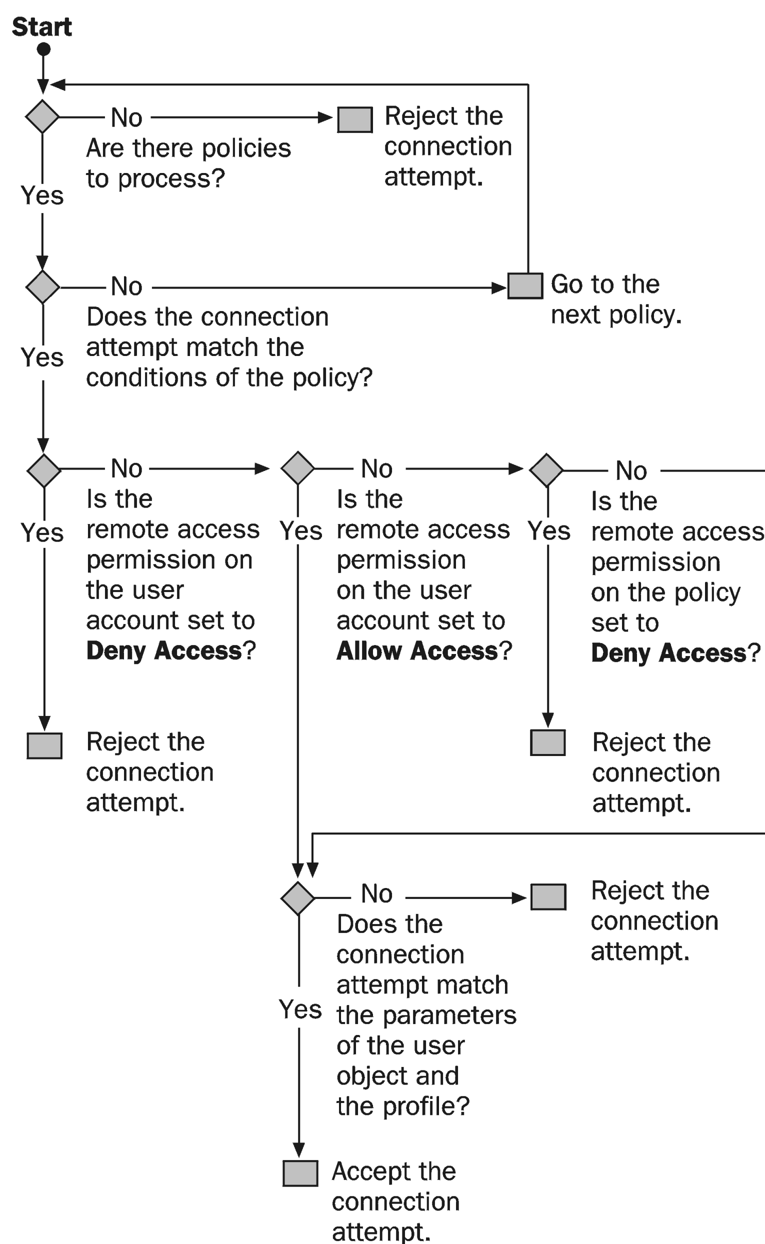
תרשים 11.5 הגדרת מדיניות גישה מרחוק

תנאים

ניתן להוסיף תנאים למדיניות גישה מרחוק (RAP) בקבוצה המפורטת של תנאים שחייבים להתמלא כדי שהמערכת תאפשר או תשלול את אפשרות לגישה מרחוק. זה עובד ביחד עם ההרשאה לגישה מרחוק המוענקת למשתמש, כדי לקבוע האם המשתמש יקבל גישה. תרשים הזרימה המוצג בתרשים 11.6 מדגים את הלוגיקה באמצעותה ניתן להסיק האם בקשת התחברות תורשה או תישלל.

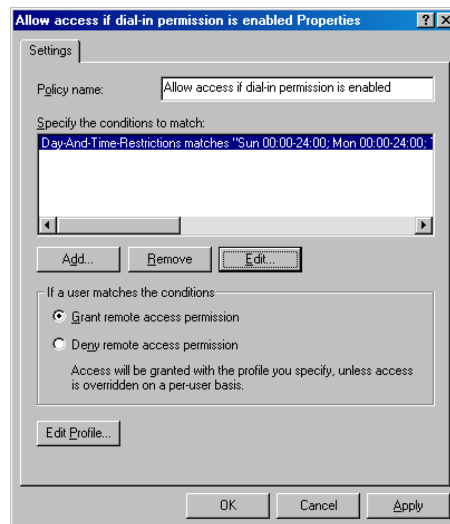
הערה אם לא קיימת מדיניות גישה מרחוק (אם לדוגמה, מדיניות ברירת המחדל נמחקה), המשתמשים לא יוכלו לקבל גישה לרשת, ללא תלות בהגדרות ההרשאה Routing and Remote Access הפרטית שלהם.

באמצעות השימוש בתרשים הזרימה, אפשר לחזות את התוצאה של בקשה להתחברות בכל מצב נתון. למשל, מאפיין החיוג פנימה של משתמש מוגדר לניהול הגישה באמצעות מדיניות גישה מרחוק (Control Access Through Remote Access Policy), ומדיניות הגישה מרחוק היא מדיניות ברירת המחדל, לאמור אפשר גישה אם ההרשאה לחיוג פנימה מאופשרת Allow Access If Dial-In Permission Is Enabled (כלומר, המדיניות הפעילה היא לשלול גישה, והתנאי הוא להרשות בכל יום, בכל שעה). אם עוקבים בתרשים הזרימה, מתברר שנסיון ההתחברות של המשתמש ייכשל.



תרשים 11.6 תרשים זרימה של מדיניות גישה מרחוק

למרות זאת, אם מאפיין החיוג פנימה של המשתמש מוגדר כ- Allow Access, אז שימוש במדיניות ברירת מחדל כמו זו הקודמת יסתיים בהתחברות מוצלחת.



תרשים 11.7 קביעת מאפייני החיוג פנימה להענקת גישה.

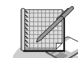
לאפשר או לשלול גישה

ניתן להגדיר מדיניות להענקת גישה או לשלילתה (Grant or Deny Access). הצירוף של מדיניות זו ושל ההרשאה לחיוג פנימה של אובייקט המשתמש תגרום לקבלת ההחלטה אם תאושר גישת המשתמש אם לאו. ההחלטה תתקבל על פי הלוגיקה המתוארת בתרשים 11.6.

Caller ID

תכונת שיחה מזוהה (Caller ID) מאמתת שהמתקשר אכן מתקשר מהמספר המצוין. אם זהות המתקשר מוגדרת, נדרשת תמיכה בהעברת נתוני זהות המתקשר כל הדרך מהמתקשר עד לשרת Routing and Remote Access, אחרת תישלל הגישה בנסיון ההתחברות.

הערה לצורך אבטחת התאימות לאחור עם גרסאות קודמות של Windows NT התכונות הבאות אינן זמינות במצב מעורב: RAP, שיחה מזוהה (Caller ID), החל נתיבים קבועים (Apply Static Routes) והקצה כתובת IP קבועה לחיבור (Assign A Static IP Address).



תרגול: יצירת מדיניות גישה מרחוק חדשה

בתרגול זה, ניצור מדיניות חדשה אשר מאפשרת גישה מרחוק המבוססת על קבוצת החברות של המשתמש.

➢ ליצירת מדיניות גישה מרחוק חדשה

1. בחלון Routing and Remote Access Manager לחץ לחיצה ימנית על Remote Access Policies, ומתפריט הקיצור בחר New Remote Access Policy.
2. הקלד שם ידידותי כגון Allow Domain Users, ולחץ Next.

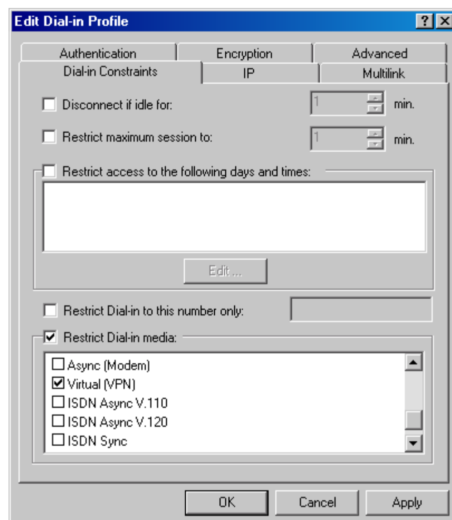
3. לחץ Add כדי להוסיף תנאי.
4. בחר Windows-groups, ולחץ Add.
5. לחץ Add, בחר Domain Users, ולחץ שוב Add. לחץ OK.
6. לחץ OK כדי לצאת מתיבת הדו-שיח Groups.
7. לחץ Next, ואז בחר ב- Grant Remote Permission.
8. לחץ Next, ולאחר מכן לחץ Finish.

הגדרת פרופיל של גישה מרחוק

הפרופיל מפרט את סוג הגישה שיקבל המשתמש אם התנאים יתאימו לנסיון ההתחברות. קיימות שש כרטיסיות שונות שיכולות לשמש להגדרת פרופיל מסוים.

Dial-In Constraints

מגבלות (Constraints) לגבי ההתחברות עצמה מוגדרות באמצעות תיבת הדו-שיח Edit Dial-In Profile בכרטיסיה Dial-In Constraints, כפי שמתואר בתרשים 11.8. הגדרות אפשריות כוללות: פרק זמן לניתוק התחברות שאינה פעילה (Idle Time Disconnect), משך זמן מירבי ל-Session (Maximum Session Time), ימים ושעות מותרים (Days And Times), מספר טלפון מורשה וסוג תווך החיוג (ISDN, תעלה, מודם אסינכרוני וכך הלאה).



תרשים 11.8 תיבת דו-שיח Edit Dial-In Profile

IP

בכרטיסיה IP מצויה ההגדרה עבור הקצאת כתובת IP ללקוח (Client IP Address Assignment) וסינון תעבורת מנות IP (IP Packet Filtering). ניתן לקבוע מסננים למנות נכנסות או יוצאות, וניתן להגדיר אותם עבור פרוטוקול IP מסוים ועבור יציאת TCP או UDP מסוימת.

Multilink

כאן תגדיר את אפשרויות ריבוי הקישורים (Multilink) ואת פרוטוקול הקצאת רוחב-פס (BAP). ניתן לנתק קו תקשורת אם רוחב הפס נופל מתחת לרמה מסוימת למשך פרק זמן נתון.

Authentication

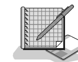
פרוטוקולי אימות, כגון PAP (**P**assword **A**uthentication **P**rotocol), CHAP (**C**hallenge **H**andshake **A**uthentication **P**rotocol), ו-EAP (**E**xtensible **A**uthentication **P**rotocol) מוגדרים כאן.

Encryption

מאפייני הצפנה (Encryption) עבור שרתי Routing and Remote Access מוגדרים בכרטיסיה זאת. אפשרויות העומדות לבחירה הן : לאסור הצפנה, להרשות אותה או לדרוש אותה.

Advanced

הכרטיסיה Advanced מאפשרת להגדיר פרמטרים נוספים הקשורים ברשת, אשר אינם ישימים לשרתי Routing and Remote Access של Microsoft. כלולות בקטגוריה זו תכונות תקניות של RADIUS ו-Ascend, אשר עשויות להיות ישימות לחומרת NAS (**N**etwork **A**ccess **S**ervers) של יצרנים אחרים.



תרגול: יצירת מסנן מדיניות

בתרגול זה תערוך את פרופיל המדיניות Allow Access If Dial-In Permission Is Enabled, כך שמשתמשים המקבלים גישה מכוח מדיניות זו לא יוכלו להפעיל את תוכנית השירות Ping (הבודקת תצורת TCP/IP ובוחנת את תקינות החיבוריות למארחי TCP/IP ברשת) ברשת של שרת Routing and Remote Access, בעוד משתמשים המקבלים גישה באמצעות המדיניות Allow Domain Users כן יכולים לעשות זאת.

➤ **כדי ליצור מסנן Echo למנות ICMP (ICPM Echo Filter) במדיניות Allow Access If Dial-In Permission Is Enabled**

1. לחץ לחיצה ימנית על מדיניות Allow Access If Dial-In Permission Enabled, ומתפריט הקיצור בחר Properties.
2. לחץ על לחצן Edit Profile.
3. בחר בכרטיסיה IP.
4. לחץ על From Client IP Packet filter.
5. לחץ Add.
6. לחץ על תיבת רשת היעד.
7. עבור כתובת ה-IP, הקלד את נתוניו של שרת Routing and Remote Access (כתובת ומסכת רשת משנה).
8. כפרוטוקול, בחר את ICMP.
9. הקלד **8** עבור ICMP Type, והקלד **0** עבור ICMP Code (ICMP סוג 8 מציין בקשה להד או Echo Request).

10. לחץ OK כדי לצאת מ- Add/Edit IP filter, ולחץ OK כדי לצאת מתיבת דו-שיח IP Packets Filters Configuration. לחץ שוב OK כדי לצאת מתיבת הדו-שיח.

הגדרת פרוטוקול הקצאת רוחב פס (BAP)

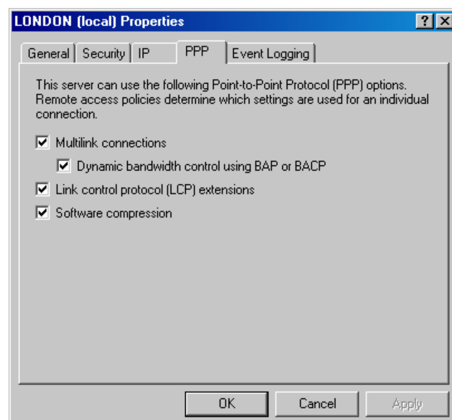
BAP (**B**andwidth **A**llocation **P**rotocol) ו-BACP (**B**andwidth **A**llocation **C**ontrol **P**rotocol) מרחיבים את Multilink על ידי הוספה או שחרור דינמי של קישורים, על פי דרישה. לעיתים, המונחים BAP ו-BACP משמשים באופן מתחלף להתייחסות לאותה פונקציונליות של רוחב פס-על-פי-דרישה. השניים הם פרוטוקולי בקרה PPP (**P**oint-to-**P**oint control **p**rotocols) ועובדים ביחד כדי לספק רוחב פס על פי דרישה.

הפונקציונליות של BAP מיושמת באמצעות: האפשרות החדשה **פרוטוקול בקרת קישור** (LCP, **L**ink **C**ontrol **P**rotocol), BACP ופרוטוקולי BAP, כפי שמתואר ברשימה בהמשך:

- **מבדיל קישורים** (Link Discriminator). אפשרות LCP חדשה המשמשת כמזהה ייחודי לכל קישור של חבילה רבת-קישורים (Multilink Bundle).
- **BACP.** פרוטוקול BACP משתמש לניהול משא ומתן של LCP, כדי לבחור Favored Peer. ה- Favored Peer משמש לקביעת איזה Peer יועדף אם ה- Peers משדרים סימולטנית את אותה בקשת BAP.
- **BAP.** פרוטוקול BAP מספק מנגנון לניהול הקישורים ורוחב הפס. ניהול הקישורים (Link Management) מאפשר הוספה ושחרור של קישורים. הדבר דורש אספקת מספרי טלפון כמו גם סוג החומרה (מודם או ISDN) של הקישורים הזמיניים הנוספים. ניהול רוחב הפס (Bandwidth Management) קובע מתי להוסיף ולשחרר קישורים, בהתבסס על השימוש בקישורים.

BAP ו-BACP מאוגדים (Encapsulated) במסגרות של פרוטוקול PPP (Point-to-Point) בשכבת קישור הנתונים (Data-Link Layer), ובהן שדה הפרוטוקול הבא (בפורמט הקסדצימלי). מידע זה עשוי להיות מועיל בעת קריאת יומני PPP. כפי שמתואר בתרשים 11.9, ניתן לאפשר בקרת הקצאת רוחב פס באמצעות BAP ו-BAPC, באמצעות הכרטיסיה PPP שבתיבת דו-שיח Connection Properties.

- C02D עבור BAP.
- C02B עבור BACP.



תרשים 11.9 הגדרת אפשרויות PPP עבור מדיניות גישה מרחוק

➢ **כדי לאפשר או לנטרל את BAP/BACP לרוחב כל השרת**

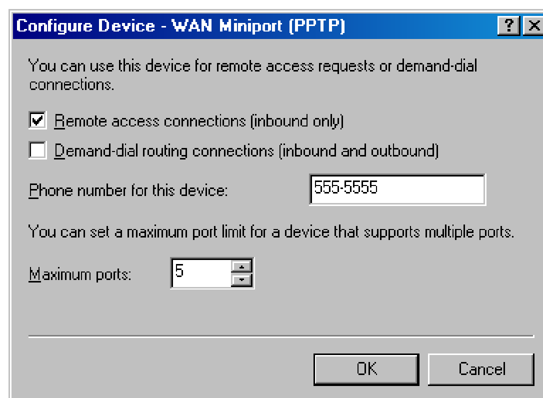
1. ב- Routing and Remote Access Manager, לחץ לחיצה ימנית על השרת בו אתה מעוניין לאפשר BAP/BACP, ומתפריט הקיצור בחר Properties.
2. בכרטיסיה PPP, סמן את תיבת הסימון Dynamic Bandwidth Control Using BAP Or BACP.

המדיניות של BAP נאכפת דרך הגדרות הפרופיל או Remote Access Policies. ניתן לגשת לערכות המדיניות Remote Access Policies באמצעות Routing and Remote Access Manager המוכר לך, או באמצעות IAS Manager.

מספרי הטלפון הנוספים של BAP

השרת יכול לספק ללקוח מספרי טלפון נוספים לחייג, במידה ונדרש רוחב פס נוסף. לשימוש באפשרות זו צריך הלקוח לדעת רק מספר טלפון אחד, אך יכול גם להפעיל קווים נוספים לפי הצורך, כפי שמתואר בתרשים 11.10.

1. ב- Routing and Remote Access Manager פתח את תפריט Ports, בחר Properties, ולחץ Configure.
2. הקלד מספרי טלפון של מודמים נוספים המיועדים לשימוש ברבוי קישורים.



תרשים 11.10 מספרי הטלפון הנוספים עבור BAP

סיכום השיעור

כאשר Routing and Remote Access כבר מותקן, הגדרנו אותו עבור התחברויות נכנסות, נעלנו אותו באמצעות RAPs, הוספנו פרופילים לגישה מרחוק לצורך אבטחה וניהלנו את הגישה בעזרת BAP.

שיעור 3: יישום ניתוב IP
ב- Remote Access Server

בשיעור זה תלמד כיצד להפוך את שרת הגישה מרחוק שלך לנתב IP, כיצד לעדכן את טבלאות הניתוב שלו, וכיצד ליישם ניתוב של חיוג-על-פי-דרישה.

לאחר שיעור זה, תוכל

- להתקין ניתוב IP (Routing and Remote Access).
- לתאר כיצד מעודכנות טבלאות ניתוב.
- ליישם ניתוב של חיוג על-פי-דרישה.

זמן לימוד משוער: 30 דקות

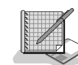
התקנת ניתוב IP

התקנת ניתוב IP דומה מאוד להתקנת שרת גישה מרחוק. למעשה, אותו האשף משמש להתקנות חדשות, כפי שמראה זאת התרגול הבא. אם כבר הותקנה אצלך גישה מרחוק, עליך לבצע את הצעדים הבאים כדי לאפשר ניתוב IP במחשב שלך.

➢ **כדי לאפשר ניתוב IP**

1. בחלון Routing and Remote Access Manager לחץ לחיצה ימנית על IP Routing, לחץ Properties, אפשר את This Computer As A Router, ולחץ OK.
2. לחץ Yes כתשובה לאזהרה: You made changes to the router configuration that require the router to be restarted. Do you want to restart now?

אם לא הותקן מראש שרת גישה מרחוק במחשב, יתווה התרגול הבא את הצעדים שיש לבצע.

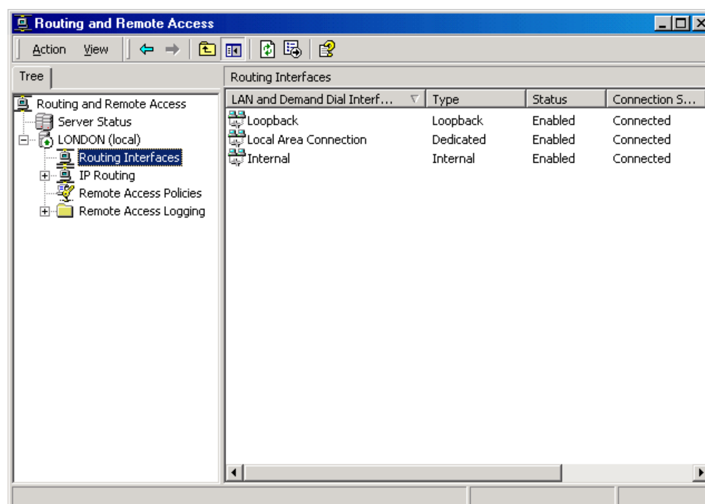


תרגול: אפשור והגדרה של Routing and Remote Access Server

במהלך תרגול זה, תתקין שרת Routing and Remote Access באמצעות Routing and Remote Access Manager (ראה תרשים 11.11).

➢ **כדי להתקין שרת Routing and Remote Access**

1. פתח את חלון Routing and Remote Access Manager.
2. לחץ לחיצה ימנית על שם המחשב שלך, ומתפריט הקיצור בחר Configure and Enable Routing And Remote Access.
3. באשף ההתקנה של Routing and Remote Access Server לחץ Next.
4. בחלון Common Configurations סמן את לחצן האפשרויות Network Router.



תרשים 11.11 ניהול שרת Routing and Remote Access

5. בדוק Remote Clients Protocol ודא שברשימת הפרוטוקולים מופיע פרוטוקול TCP/IP, ודא שהאפשרות Yes, All The Required Protocols Are On This List אכן נבחרה, ולחץ Next.

6. בחלון Demand Dial Connections ודא שנבחרה התשובה No עבור ההצעה You Can Set Up Demand-Dial Routing Connections After This Wizard Finishes, ולחץ Next.

7. לחץ Finish.

עדכון טבלאות ניתוב

החלטת הניתוב נתמכת באמצעות הידע על אילו כתובות רשת (או מזהי רשת) זמינים באגד הרשתות (Internetwork). ידע זה מרוכז במסד נתונים בשם טבלת ניתוב (Routing Table). טבלת הניתוב מורכבת מסדרות של רשומות בשם נתיבים (Routes) המכילים את המידע באשר למקום בו ממוקמות הרשתות המזוהות על ידי מזהי רשת באגד הרשתות. טבלת הניתוב אינה אקסקלוסיבית לנתב. למארחים (לא נתבים) יש גם טבלת ניתוב המשמשת לקביעת הנתיב האופטימלי.

סוגים של ערכים בטבלאות ניתוב

כל ערך בטבלת ניתוב נחשב לנתיב (route) והוא שייך לאחד הסוגים הבאים:

- **Network route.** נתיב רשת מספק נתיב למזהה רשת מסוים באגד רשתות (Internetwork).
- **Host route.** נתיב מארח מספק נתיב לכתובת אגד רשתות (Internetwork Address) המורכבת ממזהה רשת (Network ID) ומזהה מארח (Node ID). נתיבי מארח משמשים לרוב ליצירת נתיבים מותאמים למארחים מוגדרים, במטרה לנהל בקרה או

אופטימיזציה של התנועה ברשת. נתיב מארח שקול לנתיב רשת עם מסכת רשת (Netmask) 255.255.255.255.

- ❖ **Default route**. נעשה שימוש בנתיב ברירת מחדל כאשר לא נמצא נתיב אחר בטבלת הניתוב. לדוגמה, אם נתב או מארח לא מצליח למצוא נתיב רשת או נתיב מארח אל היעד, ייעשה שימוש בנתיב ברירת המחדל. נתיב ברירת המחדל מפשט הגדרת מארחים. במקום להגדיר מארחים עם נתיבים לכל מזהי הרשת המצויים באגד רשתות, נתיב ברירת מחדל בודד משמש לשליחת כל המנות עם כתובת יעד של רשת או אגד רשתות, אשר לא נמצאו בטבלת הניתוב. נתיב ברירת מחדל שקול לנתיב רשת עם מסכת רשת 0.0.0.0.

מבנה טבלת הניתוב

תרשים 11.12 מציג המבנה של טבלת ניתוב.

LONDON - IP Routing Table

Destination	Network mask	Gateway	Interface	Metric	Protocol
10.0.0.0	255.0.0.0	10.45.45.45	Local Area C...	1	Local
10.45.45.45	255.255.255.255	127.0.0.1	Loopback	1	Local
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	1	Local
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	1	Local
224.0.0.0	240.0.0.0	10.45.45.45	Local Area C...	1	Local
255.255.255.255	255.255.255.255	10.45.45.45	Local Area C...	1	Local

תרשים 11.12 טבלת ניתוב

כל ערך בטבלת הניתוב מורכב משדות המידע הבאים:

- ❖ **Destination**. מזהה הרשת או כתובת אגד רשתות עבור נתיב מארח. בנתבי IP קיים שדה נוסף של Subnet Mask הקובע את מזהה הרשת מתוך כתובת היעד.
- ❖ **Gateway**. מכיל את הכתובת אליה מועברת המנה. כתובת להעברה (Forwarding Address) היא כתובת חומרה או כתובת אגד רשתות (Internetwork). עבור רשתות בהן המארח או הנתב מחוברים באופן ישיר, שדה הכתובת להעברה עשוי להכיל את כתובת הממשק הקשור לרשת.
- ❖ **Interface**. ממשק הרשת הנמצא בשימוש כאשר המנות מועברות למזהה הרשת. זהו מספר יציאה (Port) או מזהה לוגי מסוג אחר.
- ❖ **Metric**. זו מידה לבדיקת מידת ההעדפה של הנתיב. בדרך כלל, הנתיב בעל ערך שדה מטרי הנמוך ביותר הוא הנתיב המועדף ביותר. כאשר קיימים נתיבים מרובים לרשת יעד נתונה, הנתיב עם ערך שדה מטרי הנמוך מביניהם הוא המועדף. אלגוריתמי ניתוב אחדים מאחסנים רק נתיב בודד אחד לכל מזהה רשת בטבלת הניתוב, אפילו אם קיימים נתיבים מרובים אליו. במקרה זה, הנתב משתמש בערך מטרי כדי לקבוע איזה מהנתיבים יאוחסן בטבלת הניתוב.

הערה הרשימה הקודמת אמורה להיות רשימה מייצגת של שדות הכלולים בטבלאות הניתוב המשמשות את הנתבים. השדות המעשיים, המופיעים בטבלאות הניתוב עבור פרוטוקולים ברי-ניתוב השונים, עשויים להיות שונים במקצת.

יישום ניתוב חיוג-על-פי-דרישה

ממשק לחיוג-על-פי-דרישה (Demand-Dial) הוא ממשק נתב אשר מועלה לפי דרישה בהתבסס על התנועה ברשת. קישור החיוג-על-פי-דרישה מיוזם, רק אם טבלת הניתוב מראה שהממשק נחוץ להגעה לכתובת IP יעד. טבלת הניתוב אינה מספקת פירוט כלשהו בנוגע למי או לאיזה פרוטוקול יכולים להעלות את קישור החיוג-על-פי-דרישה. הוא פשוט מבוסס על היעד אליו מופנית התנועה.

מסנני חיוג-על-פי-דרישה (Demand-Dial Filters) קובעים איזו תעבורה תיזום את קישור החיוג-על-פי-דרישה. ניתן להגדיר את המסננים לאישור או לשלילת מקורות או כתובות IP יעד, יציאות או פרוטוקולים מפורשים. שליטה רחבה יותר תושג באמצעות השימוש בהגבלת השעה-ביום. אפילו אם מתמלאים התנאים שנקבעו במסנן החיוג-על-פי-דרישה, במידה ותוטל הגבלה על שעות החיוג, באמצעות הגדרת שעות חיוג-החוצה (Dial-Out Hours), הנתב לא לחייג.

השדות המתוארים בסעיף הבא עבור כותרות IP, TCP ו-UDP יכולים לשמש להגדרת מסנני חיוג-על-פי-דרישה. Routing and Remote Access מאפשרת סינון (Filtering) על ערכים בשדות הבאים :

IP Header

צרור נתוני IP (IP Datagram) כולל כותרת IP (IP Header) באורך 20 בתים. הרשימה הבאה מתארת את שדות המפתח בכותרת IP :

- **IP Protocol.** מזהה של פרוטוקול IP הלקוח. לדוגמה, מזהה הפרוטוקול של פרוטוקול TCP הוא 6, מזהה הפרוטוקול של UDP הוא 17, ומזהה הפרוטוקול של ICMP הוא 1. שדה הפרוטוקול משמש לפירוק ריבוב OSI (Demultiplex) של מנת IP עבור פרוטוקול של השכבה מעליו (שכבת תעבורת הנתונים, Transport Layer).
- **Source IP Address.** כתובת IP המקור מאחסנת את הכתובת IP של המארח היוזם.
- **Destination IP Address.** כתובת IP היעד מאחסנת את הכתובת IP של מארח היעד. ניתן להגדיר את כתובת IP היעד בעזרת Subnet Mask, ובכך לאפשר ציון של טווח שלם של כתובות IP (הנגזרות ממזהה רשת אחד) באמצעות ערך מסנן בודד.

TCP Header

פרוטוקול TCP משתמש בתקשורות של שטף-בתים (Byte-Stream Communications) בהן המידע המוכל במקטע TCP נחשב לסדרת בתים ללא גבולות שדה או רשומה. הרשימה הבאה מתארת את שדות המפתח בכותרת TCP :

- **TCP Source Port.** יציאת מקור TCP משמשת לזיהוי תהליך המקור השולח מקטע TCP זה.

❖ **TCP Destination Port.** יציאת יעד TCP משמשת לזיהוי תהליך היעד עבור מקטע TCP זה.

UDP Header

פרוטוקול UDP משמש ליישומים אשר לא דורשים אישור קבלה (Acknowledgment) לנתונים, ואשר משדרים בדרך כלל כמויות קטנות של נתונים בבת אחת. הרשימה הבאה מתארת את שדות המפתח בכותרת UDP :

❖ **UDP source port.** יציאת מקור UDP משמשת לזיהוי תהליך המקור השולח הודעת UDP זו.

❖ **UDP destination port.** יציאת יעד UDP משמשת לזיהוי תהליך היעד עבור הודעת UDP זו.

הערה ניתן למצוא רשימת **יציאות** (Ports) **ידועות ב-** RFC 1700 **או ב-** %winroot%\system32\drivers\etc\services.

ICMP

הודעות פרוטוקול ICMP מאוגדות בצרורות נתוני IP, כך שיוכלו להיות מנותבות באגד רשתות (Internetwork). הרשימה בהמשך מפרטת שדות מפתח במנה ICMP :

❖ **ICMP type.** סוג ICMP מכיל מידע המצביע על הסוג של מנת ICMP (בקשה להד - Echo Request, או תגובה להד - Echo Reply, וכך הלאה).

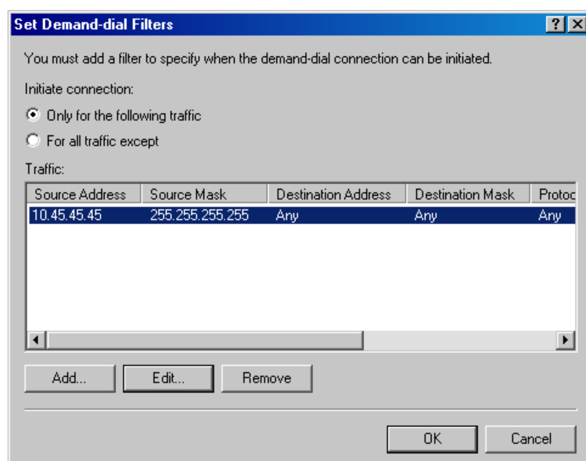
❖ **ICPM code.** קוד ICPM מצביע על אחת מתוך פונקציות מרובות האפשריות בתוך סוג ICPM נתון.

הגדרת מסנני חיוג-על-פי-דרישה

הניתוב של חיוג-על-פי-דרישה במערכת מבוססת Windows 2000 מאפשר הגדרה של מסנני חיוג-על-פי-דרישה ושעות חיוג-החוצה, כדי למנוע יצירה של התחברויות בחיוג-על-פי-דרישה.

➢ כדי להגדיר מסנני חיוג-על-פי-דרישה

1. פתח את Routing and Remote Access Manager.
2. לחץ על Routing Interfaces.
3. לחץ לחיצה ימנית על Demand-dial interface.
4. מתפריט הקיצור בחר Set Demand-Dial Filters.
5. בתיבת דו-שיח Set Demand-Dial Filters המוצגת בתרשים *11.13*, לחץ Add.



תרשים 11.13 הגדרת מסנני חיוג-על-פי-דרישה

כתובת IP מקור ויעד

כתובת IP המקור והיעד מוגדרות באמצעות Subnet Mask, המאפשרת ציון טווח שלם של כתובות IP (המתאימות לאותו מזהה רשת) באמצעות רשומת פילטר בודדת. למשל, המזהה 10.45.45.45 עם Subnet Mask 255.255.255.255 מתאים רק לכתובת אחת, בעוד 10.0.0.0 עם Subnet Mask 255.0.0.0 מתאים לרשת Class A שלמה.

פרוטוקול

פרוטוקולים שונים יכולים להיות בשימוש עבור כל פילטר:

- פרוטוקולים TCP, מבוסס-TCP ו-UDP מוגדרים עם יציאות (Ports) מקור ויעד.
- פרוטוקול ICMP מוגדר עם סוג ICMP וקוד ICMP.
- ANY פירושו פרוטוקול כלשהו.
- Other משמש לציון מזהה פרוטוקול IP. ניתן להקליד זאת כמספר או כשם של פרוטוקול. שמות פרוטוקול מתורגמים למספר פרוטוקול באמצעות הקובץ PROTOCOL שבתיקיה %winroot%\system32\drivers\etc.

פעולה

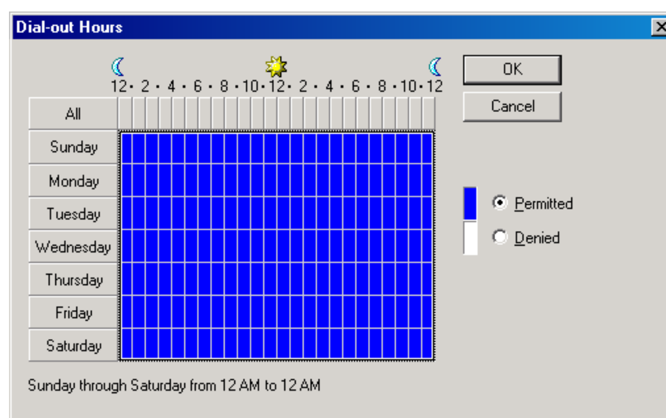
סינון החיוג-על-פי-דרישה מבוסס על חריגים (Exceptions). אתה יכול להגדיר את Routing and Remote Access ליזום התקשרות רק עבור התעבורה המוגדרת על ידי המסננים, או ליזום התקשרות עבור כל תעבורה, מלבד זו המוגדרת במסננים.

שעות חיוג-החוצה

שעות החיוג-החוצה (Dial-Out Hours) באות לפרט מתי ניתן ליצור התקשרות באמצעות חיוג-על-פי-דרישה. בעזרתן, ניתן לקבוע את השעה ביום ואת היום בשבוע בהם ההתחברות בחיוג-על-פי-דרישה מורשית או נדחית.

➢ כדי להגדיר הגבלת השעה-של-היום

1. פתח את Routing and Remote Access Manager.
2. לחץ על Routing Interfaces.
3. לחץ לחיצה ימנית על Demand-Dial Interface.
4. מתפריט הקיצור בחר Dial-Out Hours.
5. בתיבת דו-שיח Dial-Out Hours, המוצגת בתרשים 11.14, בחר את השעות (והימים) הרצויות לאישור או לשלילה.



תרשים 11.14 תיבת דו-שיח Dial-Out Hours

סיכום השיעור

בשיעור זה למדת כיצד להפוך את שרת הגישה מרחוק לנתב IP, או להתקין Routing and Remote Access, לעדכן את טבלאות הניתוב שלה ולויישם Demand-Dial Routing.

שיעור 4:
תמיכה ב- Virtual Private Networks

רשת פרטית וירטואלית (**V**irtual **P**rivate **N**etwork ,VPN) מוגדרת כיכולת לשלוח נתונים בין שני מחשבים דרך אגד רשתות (Internetwork), באופן המחקה את תכונותיה של רשת פרטית ייעודית. בשיעור זה תלמד אודות VPNs בסביבה מנותבת ובסביבת האינטרנט.

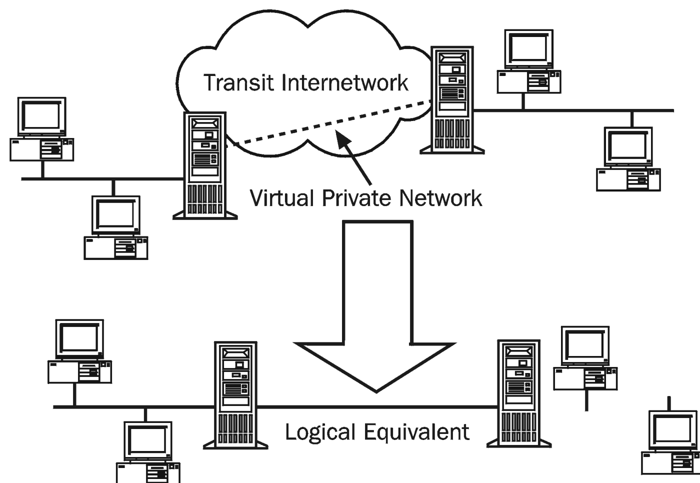
לאחר שיעור זה, תוכל

- להסביר מהי VPN.
- לתאר את VPN בסביבה מנותבת.
- לתאר שרת VPN המשולב בסביבת האינטרנט.

זמן לימוד משוער: 20 דקות

יישום VPN

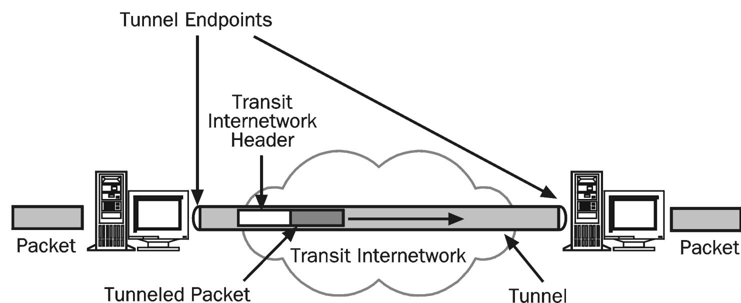
רשת פרטית וירטואלית (או VPN) מוגדרת כיכולת לשלוח נתונים בין שני מחשבים דרך אגד רשתות באופן המחקה את תכונותיה של רשת פרטית ייעודית (ראה תרשים 11.15). VPN מאפשרת למשתמשים רחוקים או ניידים להתחבר באופן מאובטח לשרת ארגוני מרוחק, תוך שימוש בתשתית הניתוב המסופקת על ידי רשת ציבורית רחבת-היקף, כגון האינטרנט. מנקודת מבטו של המשתמש, VPN הוא חיבור מנקודה-לנקודה בין מחשב המשתמש לבין השרת הארגוני. טיבעה של הרשת המתווכת (Intermediate Internetwork, שמעתה ואילך נתייחס אליה כאל רשת התעבורה, Transit Internetwork) אינו רלוונטי, מכיון שנראה כאילו הנתונים נשלחים באמצעות קישור פרטי ייעודי.



תרשים 11.15 דיאגרמת רשת פרטית וירטואלית (VPN)

טכנולוגיית VPN גם מאפשרת לארגון לתקשר עם סניפיו או עם חברות אחרות באמצעות רשת ציבורית (כגון האינטרנט) וגם לשמור על תקשורת מאובטחת. חיבור VPN דרך האינטרנט פועל לוגית כמו קישור ייעודי ברשת מרחבית (WAN).

בשני מקרים אלה, החיבור המאובטח דרך רשת התעבורה נתפס על ידי המשתמש כממשק רשת וירטואלי, המספק תקשורת של רשת פרטית באמצעות רשת ציבורית. מכאן גם נובע המונח רשת פרטית וירטואלית (Virtual Private Network).



תרשים 11.16 תעלת VPN

פעולות בסיסיות בתיעול

תיעול (Tunneling), הידוע גם בשם Encapsulation, היא שיטה לשימוש בתשתית אגד רשתות IP (IP Internetwork) כדי להעביר דרכה מטענים (ראה תרשים 11.16). המטען (Payload) יכול להיות מורכב ממסגרות (או מנות) של פרוטוקול אחר. במקום לשלוח את המסגרת כפי שהופקה על ידי הצומת המפיק (Originating Node), מאוגדת המסגרת עם כותרת נוספת. הכותרת הנוספת מספקת נתוני ניתוב, כך שהמטען המאוגד יכול לחצות את הרשת המתווכת. אז, מנותבות מנות המטען המאוגדות בין שתי נקודות הקצה של תעלה ברשת המעבר. לאחר שהמסגרות מגיעות ליעדן ברשת המעבר, מוסרת מהן הכותרת המאגדת והן מועברות ליעדן הסופי.

תהליך שלם זה (האיגוד וההעברה של מנות) מוכר בשם תיעול (Tunneling). הנתיב הלוגי דרכו מוסעות מנות המטען המאוגדות ברשת המעבר נקרא תעלה (Tunnel).

דוגמאות של תעלה

ניתן לממש תעלה באחת מהדרכים הבאות:

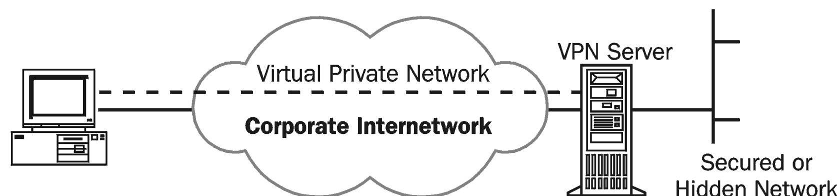
- **Point-to-Point Tunneling Protocol (PPTP).** פרוטוקול התיעול מנקודה-לנקודה PPTP מאפשר למסגרות בתעבורת IP, IPX (**I**nternetwork **P**acket E**x**change) או NetBEUI (**NetB**IOS **E**nhanced **U**ser **I**nterface) להיות מוצפנות ואז מאוגדות לצרורות עם כותרת IP, כדי להישלח דרך רשת IP ארגונית או דרך רשתות ציבוריות כגון האינטרנט.
- **Layer Two Tunneling Protocol (L2TP).** פרוטוקול התיעול של שכבת קישור הנתונים, או פשוט יותר: L2TP, מאפשר לתעבורת IP להיות מוצפנת ואז להישלח דרך כל תווך (Medium) התומך בהעברת צרורות נתונים מנקודה-לנקודה

(Point-to-Point Datagram Delivery), כגון IP, ממסור מסגרות (Frame Relay), או מצב העברה אסינכרוני (ATM, **A**synchronous **T**ransfer **M**ode).

- **IP Security (IPSec) Tunnel Mode.** מצב תיעול IPSec המאפשר למטעני IP להיות מוצפנים ומאוגדים לצרורות נתונים בכותרת IP, כדי להישלח על פני רשת IP ארגונית או רשתות ציבוריות כגון האינטרנט.
- **IP-in-IP Tunneling.** תיעול IP בתוך IP, או IP-in-IP, מאגד צרור נתוני IP קיים עם כותרת IP נוספת, המאפשר למנה לחצות רשת המאופיינת ביכולות או במדיניות חסרות קשר. שימוש נפוץ בתיעול IP-in-IP הוא ההעברת תעבורת שידור IP לרבים (Multicast Traffic) בחלקים של רשת האינטרנט, אשר אינם תומכים בניתוב שידור לרבים (Multicast Routing).

שילוב VPN בסביבה מנותבת

ברשתות ארגוניות אחדות (ראה תרשים 11.17) הנתונים של מחלקות מסוימות (כגון מחלקת משאבי אנוש) רגישים עד כדי כך, שהרשת המקומית (LAN) המחלקתית מנותקת באופן פיסי מיתר הרשת הארגונית. למרות שנוהל זה מגן על נתוני המחלקה, הוא יוצר בעיות נגישות למידע, עבור המשתמשים שאינם מחוברים פיסית לרשת המקומית הנפרדת.

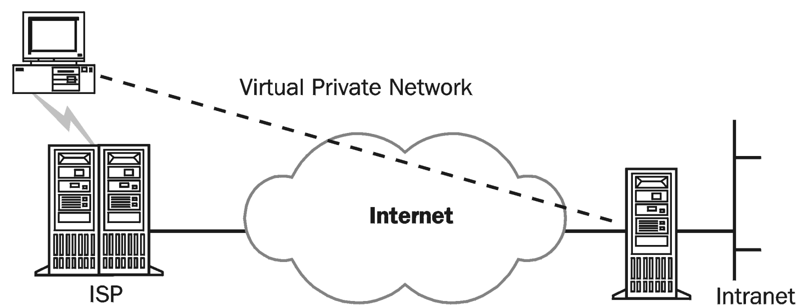


תרשים 11.17 אגד רשתות ארגונית

ה-VPNs מאפשרות ל-LAN המחלקתית להיות מחוברת פיסית לרשת הארגונית, אך מופרדת באמצעות שרת VPN. שים לב לכך, ששרת ה-VPN אינו פועל כנתב בין הרשת הארגונית וה-LAN המחלקתית. משתמשים ברשת הארגונית עם האישורים המתאימים (בהתאם למדיניות הצורך-לדעת של הארגון) יכולים להקים קישור VPN עם שרת ה-VPN ולהשיג גישה למשאבים המחלקתיים המוגנים. בנוסף לכך, כל תקשורת החוצה את קישור ה-VPN יכולה לעבור הצפנה לצורך, לשם הבטחת חסיון הנתונים. עבור אותם המשתמשים אשר אין להם אישורים מתאימים, רשת ה-LAN המחלקתית אינה ניתנת לצפייה.

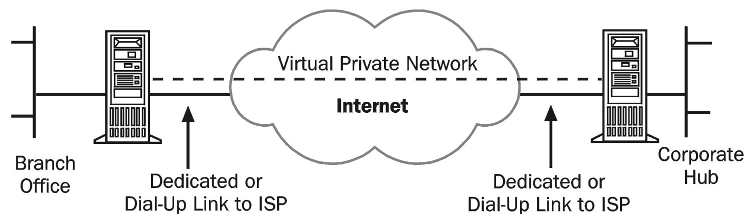
שילוב שרתי VPN בסביבת האינטרנט

לרוב, במקום שמשתמש ייזום התקשרות טלפונית ליעד מרוחק (תקשורת בינעירונית בארה״ב, או בינלאומית) או שיחת חינם 1-800, כדי לחייג לשרת גישה מרחוק לרשת הארגונית או לשרת חיצוני המשרת את הארגון (באמצעות NAS), הוא יחייג לספק שירות האינטרנט (ISP) המקומי שלו. באמצעות ההתקשרות לספק האינטרנט המקומי נוצר קישור VPN בין המשתמש המחייג לבין שרת VPN הארגוני דרך רשת האינטרנט (ראה תרשים 11.18).



תרשים 11.18 גישה מרחוק באמצעות האינטרנט

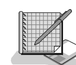
- **סניף של ארגון משתמש בקווים ייעודיים.** במקום להשתמש בשיטות הנפוצות, כגון ממסור מסגרות (Frame Relay), הן נתב רכזת הסניף והן נתב הרכזת הארגונית מחוברים לאינטרנט באמצעות תשתית קווים ייעודים מקומיים ודרך ספק שירותי אינטרנט מקומי. באמצעות החיבורים של ספק האינטרנט המקומי, נוצר קישור VPNבין נתב הסניף לבין נתב רכזת ארגון, דרך רשת האינטרנט.
- **סניף של ארגון משתמש בקו חיוג.** במקום שהנתב במשרדי הסניף יתקשר לעיל מרוחק (תקשורת בינעירונית בארה״ב, או בינלאומית), או שיחת חינם 1-800, כדי לחייג לשרת גישה מרחוק לרשת הארגונית או לשרת חיצוני המשרת את הארגון (באמצעות NAS), הוא יחייג לספק שירות האינטרנט (ISP) המקומי שלו. מההתקשרות לספק שירותי האינטרנט המקומי, נוצר קישור VPN בין נתב רכזת הסניף לבין נתב רכזת הארגון דרך האינטרנט.



תרשים 11.19 VPN באמצעות האינטרנט

הערה בשני המקרים, המשתמשים אינם מחוייבים על בסיס המרחק בין המשרדים, מפני שנעשה שימוש בקישורים פיסיים מקומיים בלבד.

כדי שחיבורי VPN יהיו זמינים בצורה אמינה, על נתב רכזת הארגון המתפקד כשרת VPN להיות מחובר לספק שירותי אינטרנט מקומי באמצעות קו ייעודי. שרת ה-VPN חייב להיות בהאזנה לקראת תעבורת VPN נכנסת במשך כל שעות היום. למרות שהדבר ניתן למימוש באמצעות התקשרות בקו חיוג, הוא פחות אמין, כיוון שלרוב נעשה שימוש בכתובות IP המוקצות באופן דינמי והחיבור המושג עלול לא להיות עקבי.

 תרגול: יצירת ממשקי VPN

במהלך התרגול, תלמד ליצור ממשקי VPN בכל נתב.

⮘ ליצירת ממשק נתב

1. פתח את Routing and Remote Access Manager, לחץ לחיצה ימנית על Routing Interfaces. מתפריט הקיצור בחר New Demand-Dial Interface, ולחץ Next.
2. תן לממשק את אותו השם כמו זה של הנתב המרוחק אליו תתחבר.
3. בחלון Connection Type בחר באפשרות Connect Using Virtual Private Network (VPN), ולחץ Next.
4. בחלון VPN Type בחר L2TP, ולחץ Next.
5. הקלד את כתובת ה-IP של הנתב המרוחק אליו תתחבר, ולחץ Next.
6. בחלון Protocols and Security, סמן את האפשרויות Route IP Packet On This Interface ו- Add A User Account So A Remote Router Can Dial In, ולחץ Next.

   תופיע תיבת דו-שיח Dial-In Credentials. זהו שם המשתמש באמצעותו יחייג הנתב המרוחק פנימה. השם מופיע מעומעם (Grayed) כיון שזהו שמו של הממשק שאתה יוצר.
7. לחץ Next.
8. הקלד את שם הנתב המקומי בתיבת דו-שיח Dial-Out Credentials. זהו שם המשתמש בו ישתמש נתב זה בעת שיתחבר לנתב המרוחק. שם משתמש זה יתאים לשם של ממשק חיוג-על-פי-דרישה בנתב המרוחק. השאר Domain and Password ללא מילוי, ולחץ Next.
9. לחץ Finish.
10. חזור על צעדים 1 עד 9 עבור הנתב האחר.

הערה כאשר יוצרים תעלה נתב-לנתב באמצעות רשת ציבורית, יש להגדיר את המסננים בממשקי נתב החיצוניים לאפשור של התנועה המתועלת בלבד.

⮘ להחלפת נתיבים תוך שימוש בעדכון Auto Static

1. בחלון Routing and Remote Access Manager הרחב את IP Routing, ולחץ על General.
2. לחץ לחיצה ימנית על Demand-Dial Interface, ומתפריט הקיצור בחר Update Routes.
3. חזור על צעדים 1 ו- 2 בנתב האחר.

⮘ כדי לצפות בנתיבים שהתקבלו במשך עדכון ה-Auto Static

1. בחלון Routing and Remote Access Manager לחץ IP Routing ו- Static Routes.

➢ כדי לנסות את התעלה

1. מהנתב מספר 1, הפעל משורת הפקודה (Command Prompt) את תוכנית השירות PING על הכתובת IP של הנתב מספר 2.

תעלת החיוג-על-פי-דרישה צריכה להיווצר ופעולת ה-PING להצליח.

סיכום השיעור

רשת פרטית וירטואלית (VPN) מוגדרת כיכולת לשלוח נתונים בין שני מחשבים על פני אגד רשתות, בצורה המחקה את התכונות של רשת פרטית ייעודית. בשיעור זה, למדת על VPNs בסביבה מנותבת ועל פני האינטרנט.

שיעור 5: תמיכה בקישורי Multilink

טכנולוגיית **ריבוי הקישורים (Multilink)** הוכנסה לראשונה ב- Remote Access Service של Windows NT 4.0. היא מאפשרת שילוב של קישורים פיסיים מרובים בקישור לוגי יחיד. בצורה אופיינית, שניים או יותר קווי ISDN או קישורי מודם מצורפים יחד, במטרה להגדיל את רוחב הפס של החיבור. בשיעור זה יוסבר נושא Multilink.

לאחר שיעור זה תוכל

- להסביר מהם חיבורי Multilink.

זמן לימוד משוער: 10 דקות

פרוטוקול נקודה-לנקודה (PPP)

פרוטוקול נקודה-לנקודה, או בשמו הנפוץ PPP (**P**oint-to-**P**oint **P**rotocol), פותח כדי לשלוח נתונים דרך חיבורי נקודה-לנקודה באמצעות קווי חיוג או קווים ייעודיים. PPP מאגד (Encapsulates) מנות IP, IPX ו-NetBEUI בתוך מסגרות PPP, ואז משדר אותן דרך קישור נקודה-לנקודה. PPP יכול לשמש בין נתבים באמצעות קישורים ייעודיים, או בין לקוח שירות גישה מרחוק והשרת, באמצעות קישורים בחיוג. PPP מורכב משלוש הפונקציות העקריות או רכיבים הבאים :

- **Encapsulation.** האיגוד מאפשר ריבוב של מספר פרוטוקולי העברה על אותו קישור.
- **LCP.** פרוטוקול PPP מגדיר LCP בר הרחבה (Extensible **L**ink **C**ontrol **P**rotocol) המשמש להקמה, הגדרה ובחינה של החיבור ברמת קישור הנתונים (Data-Link Layer). LCP המורחב מספק גם את הטיפול בלחיצת-היד (Handshake) עבור פורמט האיגוד, גודל המנה, יצירת או ניתוק הקישור ואימות (החלפת האישורים). דוגמאות אחדות של פרוטוקולי אימות כוללות PAP, CHAP ו-EAP.
- **Network Control Protocol.** פרוטוקולים לבקרת הרשת (NCPs) מספקים צרכי הגדרה מסוימים המותאמים לפרוטוקולי התעבורה שלהם. לדוגמה, IPCP הוא פרוטוקול בקרת IP (IP Control Protocol).

הערה ניתן למצוא מידע נוסף לגבי PPP ו-Multilink במסמך RFC 1661: The Point-to-Point Protocol ובמסמך RFC 1990: PPP Multilink.

Multilink PPP

ריבוי קישורים (Multilink) הוכנס לראשונה ב- Remote Access Service של Windows NT 4.0. הוא מאפשר שילוב של קישורים פיסיים מרובים בקישור לוגי יחיד. בדרך כלל, מאגדים שניים או יותר קווי ISDN או קישורי מודם, במטרה להגדיל את רוחב הפס. תמיכה ב-Multilink מיושמת באמצעות :

- **אפשרות LCP חדשה.** היכולת לתמוך ב-Multilink מוסדרת במשא ומתן במהלך שלב LCP של פרוטוקול PPP.

❖ **פרוטוקול רשת PPP חדש.** פותח פרוטוקול רשת PPP חדש הנקרא MP (**M**ultilink **P**PP). MP נראה ל-PPP כמטען PPP רגיל. פרוטוקול MP יבצע סידור וצירוף חוזרים (Resequence and Recombine) של מנות לפני העברתן לטיפולו של פרוטוקול התעבורה המעשי, כגון TCP/IP.

MP מאוגד במסגרות PPP של שכבת Data-Link עם שדה הפרוטוקול בעל ערך הקסדצימלי של 003D. מידע זה עשוי להיות מועיל בעת קריאת יומני PPP.

סיכום השיעור

Multilink הוכנסה לראשונה ב-Windows NT 4.0 Remote Access Service . היא מאפשרת צירופם של קישורים פיסיים מרובים לקישור לוגי אחד. בדרך כלל, מאוגדים שניים או יותר קווי ISDN או קישורי מודם, לקבלת רוחב פס גדול יותר.

שיעור 6: שימוש בניתוב וגישה מרחוק עם שירות DHPC

כאשר מאגר הכתובות של Routing and Remote Access מוגדר לשימוש ב-DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol), אין פירושו של דבר שמנות DHCP כלשהן ינועו דרך החיבורים אל לקוחות שירות Routing and Remote Access. בשיעור זה תלמד כיצד מטפל Routing and Remote Access ב-DHCP.

לאחר שיעור זה, תוכל

- להסביר את השילוב בין Routing and Remote Access לבין DHCP.
- לתאר כיצד ליישם את סוכן הממסר של DHCP.

זמן לימוד משוער: 10 דקות

ניתוב וגישה מרחוק עם DHCP

כאשר מאגר הכתובות של Routing and Remote Access מוגדר לשימוש ב-DHCP, אין פירושו של דבר שמנות DHPC כלשהן ינועו דרך החיבורים אל לקוחות שירות Routing and Remote Access. Routing and Remote Access עושה שימוש ב-DHCP כדי לחכור כתובות בבלוקים של 10 כתובות, ומאחסן אותן ברישום המערכת (Registry). מרכז המידע של הרשת (NIC, **N**etwork **I**nformation **C**enter) המשמש לחכירת כתובות DHCP אלו, ניתן להגדרה מממשק המשתמש אם קיימים בשרת שני NICs או יותר. בגירסאות קודמות של Windows, היה שרת ה- Remote Access Service מחדש ומתחזק את כתובות DHCP אלו לעד. ב- Windows 2000, חכירות DHCP משוחררות (Released) כאשר שירות ה- Routing and Remote Access נסגר.

מספר הכתובות ש- Routing and Remote Access יחכור בבת אחת ניתן להגדרה באמצעות מפתח הרישום (Registry Key):

\System\CurrentControlSet\Services\RemoteAccess\Parameters\Ip\InitialAddressPoolSize

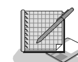
הערך במפתח זה הוא מספר חכירות DHCP ש- Routing and Remote Access ישמור בהתחלה. כתובות אלו מאוחסנות ברישום המערכת והן מוקצות ללקוחות ניתוב וגישה מרחוק. כאשר המאגר ההתחלתי מתרוקן, ייחכר גוש חדש באותו הגודל.

סוכן הממסר של DHCP

סוכן הממסר (Relay Agent) של DHCP יכול לעבוד כיום באמצעות Routing and Remote Access. לקוח Routing and Remote Access יקבל כתובת IP משרת Routing and Remote Access, אך יכול להשתמש במנות DHCPINFORM כדי להשיג כתובות WINS ו- DNS, שם Domain או אפשרויות DHCP אחרות. הודעות DHCPINFORM משמשות להשגת מידע על האפשרויות, מבלי לקבל כתובת IP.

הערה שליחת שם ה-Domain תוך שימוש ב-DHCPINFORM היא בעלת חשיבות מיוחדת, כיון ש-PPP אכן יכלול אינפורמציה זאת בהגדרותיו.

כתובות DNS ו-WINS המתקבלות תוך שימוש ב-DHCPINFORM ייאכפו (Override) על הכתובות שהושגו משרת ה-RRAS.



תרגול: הגדרת סוכן ממסר DHCP לעבודה באמצעות Routing and Remote Access

כדי להגדיר סוכן ממסר DHCP

1. ב-Routing and Remote Access Manager לחץ על IP Routing, לחץ לחיצה ימנית על General, ומתפריט הקיצור בחר New Routing Protocol.
2. בחר באפשרות DHCP Relay Agent, ולחץ OK.
3. סמן את DHCP Relay Agent, ולחץ לחיצה ימנית עליו. מתפריט הקיצור בחר Properties.

   תופיע תיבת דו-שיח DHCP Relay Agent Properties, בה תוכל להגדיר את כתובות ה-IP של שרת DHCP כלשהו.
4. לחץ OK כדי לסגור את תיבת דו-שיח DHCP Relay Agent Properties.
5. לחץ לחיצה ימנית על DHCP Relay Agent, ומתפריט הקיצור בחר New Interface.
6. בחר באפשרות Internal (Internal מסמל את הממשק הווירטואלי המחובר לכל לקוחות Routing and Remote Access), ולחץ OK.
7. לחץ OK כדי לאשר ולסגור את תיבת דו-שיח DHCP Relay Agent Internal Properties.

סיכום השיעור

כאשר מאגר הכתובות של Routing and Remote Access מוגדר לשימוש ב-DHCP, אין פירושו של דבר שמנות DHPC כלשהן ינועו דרך החיבורים אל לקוחות Routing and Remote Access. בשיעור זה למדת כיצד מטפל Routing and Remote Access ב-DHCP ובסוכן הממסר של DHCP.

שיעור 7: ניהול וניטור בגישה מרחוק

ניתן לנהל ולנטר שרת גישה מרחוק בעזרת כמה כלים. בשיעור זה תלמד אודות ניהול יומן גישה מרחוק, ניהול חשבונות, Netsh, Network Monitor ותוכניות שירות אחרות מה- Resource Kit.

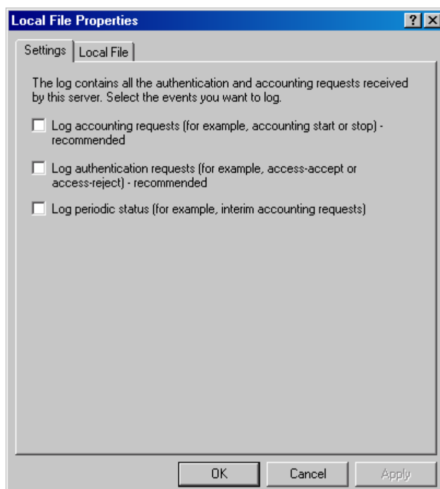
לאחר שיעור זה, תוכל

- להסביר את ניהול יומן הגישה מרחוק.
- לתאר את נושא ניהול החשבונות.
- להסביר Netsh.
- להבין את תפקידו של Network Monitor בגישה מרחוק.
- למנות חלק מתוכניות השירות לניטור גישה מרחוק.

זמן לימוד משוער: 30 דקות

רישום יומן של בקשות אימות משתמש וניהול חשבון

שירות אימות האינטרנט (IAS, **I**nternet **A**uthentication **S**ervice) של Windows 2000 יכול ליצור קבצי רישום (יומנים) המבוססים על בקשות האימות וניהול החשבון, אשר התקבלו משרת הגישה לרשת (NAS, **N**etwork **A**ccess **S**erver). הדבר אפשרי באמצעות איסוף וריכוז של מנות אלו במיקום אחד. הגדרת קבצי יומן כאלה והשימוש בהם למעקב אחר נתוני האימות, כגון כל כניסה, כל דחיית כניסה וכל נעילת חשבון אוטומטית, יכולים לעזור לפשט את ניהול שירות הניתוב והגישה מרחוק. אפשר גם להגדיר קבצי יומן ולהשתמש בהם למעקב אחר נתוני ניהול החשבונות, כגון רישומי התחברות והתנתקות, כדי לאפשר ניהול חשבונות למטרות חיוב (ראה תרשים 11.20).



תרשים 11.20 הגדרת קבצי יומן ל- Remote Access

כאשר אתה מגדיר קבצי יומן, תוכל לפרט:

- ❖ סוג הבקשות שיש לרשום.
- ❖ פורמט הקובץ של היומנים.
- ❖ התדירות בה מתחילים יומנים חדשים.
- ❖ המקום בו יאוחסנו היומנים.

ניתן גם לבחור את סוגי הבקשות שיש לרשום, מבין המתקבלות על ידי שרת ה-IAS:

❖ **בקשות לניהול החשבונות:**

- ✸ בקשות לפתיחת ניהול החשבונות, הנשלחות על ידי שרת ה-NAS, כדי לציין שה-NAS מחובר במצב מקוון ומוכן לקבל התחברויות.
- ✸ בקשות לסגירת ניהול החשבונות, הנשלחות על ידי שרת ה-NAS, כדי לציין שה-NAS עומד להתנתק (לעבור למצב Offline).
- ✸ בקשות להתחלת ניהול חשבון, הנשלחות על ידי שרת ה-NAS (לאחר שהמשתמש התקבל על ידי שרת ה-IAS המאשר), כדי לציין תחילתו של שיח משתמש (User Session).
- ✸ בקשות להפסקת ניהול חשבון, הנשלחות על ידי שרת ה-NAS, כדי לציין סיומו של שיח משתמש.

❖ **בקשות אימות:**

- ✸ בקשות אימות הנשלחות על ידי שרת ה-NAS בשם המשתמש המתחבר. ערכי רישום אלה מכילים רק מאפיינים נכנסים.
- ✸ אישורי אימות או דחיות, הנשלחים על ידי שרת ה-IAS אל שרת NAS כדי לציין אם יש לקבל או לדחות את המשתמש. ערכי רישום אלה מכילים רק מאפיינים יוצאים.
- ✸ מצב מחזורי, כדי להשיג בקשות לניהול חשבון-ביניים הנשלחות על ידי שרתי NAS אחדים במהלך שיחים.
- ✸ בקשות לניהול חשבון-ביניים, הנשלחות על ידי שרת NAS באופן מחזורי (אם אכן מוגדרת תכונת פרק זמן לניהול חשבון ביניים (Acct-Interim-Interval) לתמיכה בבקשות מחזוריות, בפרופיל גישה מרחוק בשרת IAS).

בהתחלה, מומלץ שתבחר רק בשתי האפשרויות הראשונות, ותעדן את שיטות הרישום שלך רק לאחר שתקבע אילו נתונים מתאימים ביותר לצרכיך.

כשמגדירים את השרתים המקומיים, יש לפרט האם מתחילים יומנים חדשים בתדירות יומית, שבועית, חודשית, או כשהיומן מגיע לגודל מפורט. אפשר גם לפרט שיומן אחד ויחיד מנוהל באופן רציף (ללא תלות בגודל הקובץ), אך הדבר אינו מומלץ. המוסכמה למתן שמות ליומנים נקבעת על פי מחזור הרישום שתבחר בו. מכיון ששינוי באפשרות זו יכול לגרום לכתיבה דורסת על יומנים קיימים, רצוי להעתיק את היומנים לקובץ נפרד לפני שמשנים את אורך מחזור הרישום של היומנים. על פי ברירת מחדל, קבצי

הרישום (יומן) ממוקמים בתיקיה %systemroot%\system32\LogFiles, אך תמיד קיימת האפשרות לציין מקום חילופי עבורם.

רשומות קובץ יומן

המאפיינים רשומים בפורמט UTF-8 (**U**nicode **T**ranslation **F**ormat-**8**) ומקודדים בפורמט של ערכים מופרדים על ידי פסיקים (Comma-Delimited Format). הפורמט של הרשומות בקובץ יומן תלוי בפורמט הקובץ.

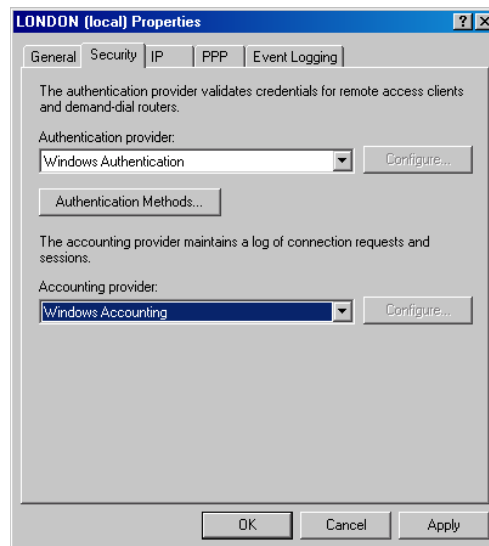
- בקבצי יומן מפורמטי-IAS, כל רשומה מתחילה בכותרת בעלת פורמט Fixed המורכבת מכתובת ה-IP של שרת NAS, שם משתמש, תאריך הרשומה, שעת הרשומה, שם השירות ושם המחשב, ואחרי הכותרת עוקבים זוגות של ערכי התכונות (שדות הרשומה).
- בקבצי יומן המיובאים ממסד נתונים, כל רשומה מכילה ערכי תכונות המסודרים ברצף עקבי המתחיל בשם המארח, שם השירות, תאריך מוטבע ושעה מוטבעת ברשומה. שרת NAS עשוי שלא להשתמש בכל התכונות המפורטות בפורמט יומן המיובא ממסד נתונים, אך המיקום התחום בפסיקים (Comma-Delimited Location) עבור כל אחת מהתכונות המוגדרות מראש נשמר בקביעות, אפילו עבור תכונות אשר איו להן ערך מפורט ברשומה.

ניהול חשבונות

ניתן להגדיר את RRAS לרישום נתונים חשבונאים במקומות הבאים:

- קבצי רישום המאוחסנים באופן מקומי לאחר שהוגדרו עבור חשבונאות Windows. מהות המידע הרשום ומקום אחסונו מוגדרים באמצעות מאפייני התיקיה Remote Access Logging ב-Snap-In של Routing and Remote Access.
- בשרת RADIUS המוגדר עבור חשבונאות RADIUS. אם שרת ה-RADIUS הוא שרת IAS, קבצי היומן מאוחסנים בשרת ה-IAS. מהות המידע הרשום ומקום אחסונו מוגדרים באמצעות מאפייני התיקיה Remote Access Logging ב-Snap-In של Internet Authentication Service.

הגדרת ספק החשבונאות עבור RRAS נעשית בכרטיסיה Security, ממאפייני Remote Access Router ב-Snap-In של Routing and Remote Access, כמו בתרשים 11.21, או באמצעות הכלי Netsh.



תרשים 11.21 הגדרת ספק החשבונאות עבור Remote Access

תוכנית השירות של שורת-הפקודה Netsh

Netsh (Net Shell) היא תוכנית שירות של שורת הפקודה וכלי לכתיבת תסריטים עבור רכיבי רשת של Windows 2000 במחשבים מקומיים או מרוחקים. Netsh מסופקת עם Windows 2000. Netsh גם מסוגלת לשמור תסריט הגדרה (Configuration Script) בקובץ טקסט למטרות ארכיון, או כדי להגדיר שרתים אחרים.

Netsh היא מעטפת (Shell) המסוגלת לתמוך ברכיבי Windows 2000 מרובים, על ידי הוספת ספריות קישור דינמיות מסייעות (Netsh Helper DLLs). DLL המסייע ל-Netsh, מרחיב את הפונקציונליות של Netsh על ידי אספקת פקודות נוספות לניטור או הגדרת תצורה של רכיב רשת ספציפי של Windows 2000. כל DLL המסייע ל-Netsh מספק הקשר (Context), לאמור: קבוצת פקודות עבור רכיב רישות ספציפי. בתוך כל הקשר יכולים להתקיים הקשרי-משנה (Subcontexts). לדוגמה, בתוך הקשר הניתוב (Routing Context), קיימים הקשרי-המשנה IP ו-IPX, כדי לקבץ את פקודות ניתוב IP וניתוב IPX יחד.

עבור Routing and Remote Access יש ל- Netsh הקשרים הבאים:

- **Ras.** השתמש בפקודות בהקשר ras כדי להגדיר תצורה של גישה מרחוק.
- **Aaaa.** השתמש בפקודות בהקשר aaaa כדי להגדיר תצורה של רכיב AAAA, המשמש את Routing and Remote Access וגם את IAS.
- **Routing.** השתמש בפקודות בהקשר routing כדי להגדיר ניתוב IP וניתוב IPX.
- **Interface.** השתמש בפקודות בהקשר interface כדי להגדיר ממשקים של חיוג-על-פי-דרישה.

Network Monitor

Network Monitor מאפשר לאתר ולאבחן בעיות ברשתות מקומיות (LANs) וברשתות מרחביות (WANs), כולל קישורי Routing and Remote Access. תוכנית השירות Network Monitor מאפשרת לזהות תבניות תעבורה ברשת, ולאתר בעיות רישות. לדוגמה, ניתן לאתר בעיות בהתקשרות שרת/לקוח, למצוא מחשב המעלה מספר בלתי סביר של בקשות עבודה, ללכוד מסגרות (מנות) ישירות מהרשת, להציג ולסנן את המסגרות שנלכדו ולזהות משתמשים לא מורשים ברשת הארגון. לקבלת מידע נרחב יותר אודות Network Monitor, ראה פרק 4.

ערכת עזרי שירות

תוכניות השירות הבאות הן חלק מערכת עזרים המקלים על עבודת הניהול והניטור של Routing and Remote Access.

RASLIST.EXE

תוכנית שורת-הפקודה RASLIST.EXE מציגה הודעות שרת Routing and Remote Access מהרשת. Raslist מאזינה להודעות שרת Routing and Remote Access בכל כרטיסי הרשת הפעילים במחשב בו היא מופעלת. פלט התוכנית מראה איזה כרטיס קיבל את ההודעה. Raslist היא כלי ניטור. יכולות לחלוף כמה שניות עד שהנתונים מתחילים להופיע; הנתונים ימשיכו להופיע עד שהתוכנית מופסקת.

RASSRVMON.EXE

RASSRVMON.EXE מאפשרת לנטר את פעולות שרת הגישה מרחוק בשרת שלך, בפירוט גדול יותר מזה שהכלים התקניים של Windows מאפשרים. Rassrvmon מספקת את נתוני הניטור הבאה:

- מידע על השרת כגון שעת הקריאה הראשונה לשרת, שעת הקריאה האחרונה לשרת, סך כל הקריאות, סך כל הבתים המועברים דרך שרת, ספירת התקשרויות בשיא, סך כל זמן ההתקשרויות, משתמשים מחוברים בכל רגע נתון ומידע לגבי ההתקשרות שלהם.
- מידע לפי יציאה (Port), שהוא שעת הקריאה הראשונה ליציאה, שעת הקריאה האחרונה ליציאה, סך כל התקשרויות ליציאה זו מאז ומתמיד, סך כל הבתים המועברים ביציאה זו, סך כל השגיאות ביציאה זו ומצבה הנוכחי של היציאה.
- מידע מסכם, כגון סטטיסטיקות, שמור עבור כל צירוף ייחודי משתמש/מכונה מאז תחילת הניטור: סך כל זמן ההתקשרות, סך כל הבתים המשודרים, ספירת התקשרויות, זמן התקשרות ממוצע וספירת סך כל השגיאות.
- מידע על התקשרויות הפרט, הכולל סטטיסטיקות לפי-התקשרות עבור כל התקשרות: שם המשתמש/שם המחשב, כתובת IP, זמן להקמת ההתקשרות, אורך משך ההתקשרות, בתים מועברים, ספירת שגיאות ומהירות הקו.

לשם הגמישות, ניתן להגדיר את התוכנית שתתריע במקרה הצורך. בדרך זו תוכל לבצע התרעה על ידי שליחת הודעת דואר אלקטרוני, שליחת הודעה לזימונית, הקפצת הודעה על מסך משתמש מוגדר, או כל פעולה אחרת שתמכן עם קובץ הפעלה או תסריט אצווה.

RASUSERS.EXE

תוכנית המאפשרת לך להציג את כל חשבונות המשתמש (ב-Domain או בשרת) שקיבלו הרשאה לחיוג פנימה אל הרשת באמצעות Routing and Remote Access, תכונות Windows 2000 אשר מיישמת את נושא הגישה מרחוק.

TRACEENABLE.EXE

TRACEENABLE.EXE הוא כלי מבוסס-ממשק משתמש גרפי, המאפשר עיקוב ומציג אפשרויות לעיקוב הנוכחי. ל- Routing and Remote Access של Windows 2000 יש יכולת עיקוב נרחבת אשר ניתן לגייסה, לשם אבחון בעיות רשת מורכבות. העיקוב רושם משתנים של מרכיבים פנימיים, קריאות לפונקציות ואינטראקציות. ניתן לאפשר באופן עצמאי לרכיבים נפרדים של Routing and Remote Access את רישום נתוני עיקוב בקבצים (עיקוב קבצים, File Tracing). יש לאפשר את פונקציית העיקוב על ידי החלפת ההגדרות ברישום של Windows 2000, תוך שימוש ב-TRACEENABLE.EXE.

שימוש ב- TRACEENABLE.EXE

בזמן שכל פריט עיקוב נבחר בתיבה המעורבת, מוצגים הערכים. בצע את השינויים שלך, ולחץ Set. לחיצה זו רושמת את השינויים שביצעת לרישום המערכת (Registry). כדי להשיג עיקוב ב-MMC, עליך להפעיל אותו עבור הרכיב ולבצע הפעלה באמצעות תיבת סימון ה-master בחלק העליון של חלון Traceenable. לדוגמה, כדי ליצור קובץ יומן עבור PPP :

1. בחר PPP מהרשימת הנפתחת.
2. לחץ Enable File Tracing.
3. לחץ Set.

עיקוב מאופשר כעת עבור רכיב זה. ברוב המקרים, קובץ היומן נוצר ב- %windir%\tracing .

סיכום השיעור

ניתן לנהל ולנטר שרת גישה מרחוק בעזרת כמה כלים. בשיעור זה, למדת על ניהול היומן וניהול החשבונות להתחברויות בגישה מרחוק, על Netsh תוכנית השירות עבור רכיבי הרשת של Windows 2000, על Network Monitor ועל תוכניות שונות המרכיבות ערכת עזרי שירות.

שאלות סיכום

השאלות הבאות נועדו לחזק את הנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות על שאלה, עיין בשיעור המתאים ונסה את השאלה שנית. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואחר כך בעברית.

Answering the following questions will reinforce key information presented in this chapter. If you are unable to answer a question, review the appropriate lesson and then try the question again. Answers to the questions can be found in Appendix A, "Questions and Answers."

1. What is a VPN?
2. Demand-dial filters can screen traffic based on what fields of a packet?
3. True or false: When setting dial-in user permissions (Allow Access, Deny Access) through the User Property page, RAPs are not used.
4. True or false: DHCP packets are never sent over Routing and Remote Access links.
5. What is the function of BAP?

1. מהו VPN?
2. מסנני חיוג-על-פי-דרישה יכולים לסנן תעבורה בהתבסס על איזה מבין שדות המנה?
3. נכון/לא נכון: בהגדרת הרשאות למשתמש בחיוג פנימה (Allow Access / Deny Access) דרך חלון ה- User Property, ערכות מדיניות של גישה מרחוק (RAPs) לא באות לידי שימוש.
4. נכון/לא נכון: מנות DHCP מעולם אינן נשלחות באמצעות קישורי Routing and Remote Access.
5. מהו תפקידו של BAP?

פרק 12

תמיכה ב-NAT

אודות פרק זה

Network **A**ddress **T**ranslation (NAT) הוא פרוטוקול המאפשר לרשת של כתובות פרטיות לגשת למידע הנמצא ברשת האינטרנט באמצעות תהליך תרגום של פרוטוקול IP. בפרק זה תלמד כיצד להגדיר רשת משרדית קטנה, או אפילו ביתית, להשתמש בחיבור אינטרנט יחיד באמצעות NAT.

לפני שתתחיל

להשלמת פרק זה עליך :

- להשלים את פרק 10.

שיעור 1: הכרת NAT

NAT מאפשר לרשת של כתובות IP פרטיות (Private IP Addresses) להיות מתורגמות לכתובות IP ציבוריות לצורך תעבורה אל ומאת האינטרנט. תרגום זה מונע מהתעבורה לעבור ישירות לרשת הפנימית, בעודו חוסך מבעלי הרשת הביתית או המשרדית את העלויות והזמן הכרוכים בהשגה וניהול של טווח כתובות ציבוריות. שיעור זה מספק סקירה אודות NAT.

לאחר שיעור זה, תוכל

- לתאר את מטרת NAT.
- לזהות את רכיבי NAT.
- לתאר את אופן פעולתו של NAT.

זמן לימוד משוער: 45 דקות

תרגום כתובות רשת

NAT (**N**etwork **A**ddress **T**ranslation) של Windows 2000 מאפשר למחשבים ברשת קטנה, כגון משרד קטן או ביתי, לשתף חיבור אינטרנט יחיד וכתובת ציבורית יחידה. המחשב בו מותקן NAT יכול לשמש גם כמתרגם כתובת רשת, שרת DHCP בזעיר אנפין, Proxy של DNS ו-Proxy של WINS. NAT מאפשר למחשבים מארחים לשתף כתובת IP ציבורית רשומה אחת או יותר, ובכך לחסוך בכתובות ציבוריות.

הבנת NAT

עם NAT בסביבת Windows 2000 תוכל להגדיר את הרשת הביתית או המשרדית שלך לשתף חיבור יחיד לאינטרנט. NAT כולל את הרכיבים הבאים:

- **רכיב התרגום.** נתב Windows 2000 בו מאופשר NAT, ואשר ייקרא מעתה ואילך מחשב NAT, מתפקד כמתרגם כתובות רשת. הוא מתרגם את כתובות ה-IP ואת מספרי יציאות המנות של TCP/UDP אשר מועברות בין הרשת הפרטית לציבורית.
- **רכיב המיעון.** מחשב NAT מספק נתוני תצורת כתובת IP למחשבים האחרים ברשת הביתית. רכיב המיעון (Addressing Component) הוא שרת DHCP בזעיר אנפין המקצה כתובת IP, Subnet Mask, Default Gateway וכתובת IP של שרת DNS. עליך להגדיר את המחשבים ברשת הביתית כלקוחות DHCP, כדי שיקבלו את הגדרות ה-IP באופן אוטומטי. תצורת ברירת המחדל של TCP/IP עבור מחשבי Windows 2000, Windows NT, Windows 95 ו- Windows 98 היא כלקוחות DHCP.

- **רכיב הסדרת שמות.** מחשב NAT הופך להיות גם שרת ה-DNS עבור מחשבים אחרים ברשת ביתית. כאשר מתקבלת בקשה להסדרת שם (Name Resolution Request) במחשב NAT הוא מעביר את הבקשה לשרת DNS האינטרנטי המוגדר בו, ומחזיר את התגובה למחשב ברשת הביתית.

חיבורי אינטרנט מתורגמים ומנותבים

קיימים שני סוגי חיבורים לאינטרנט: **מנותבים** (Routed) **ומתורגמים** (Translated). כאשר מתכננים חיבור מנותב תצטרך לקבל מספק שירותי האינטרנט (ISP) שלך טווח (Range) של כתובות IP בו תוכל להשתמש בחלק הפנימי של הרשת, והוא גם יספק לך כתובת IP של שרת DNS בו עליך להשתמש. תוכל להגדיר את כתובות ה-IP במחשבי הרשת באופן ידני (סטטי) או להשתמש בשרת DHCP.

בנתב Windows 2000 צריך להיות מוגדר כרטיס רשת עבור הרשת הפנימית (10 או 100BaseT Ethernet, למשל). בנוסף צריך להיות מוגדר בו חיבור חיצוני לאינטרנט, כגון מודם אנלוגי או מתאם ISDN, מתאם xDSL, מודם כבלים או קו T1 חכור.

השיטה המתורגמת, או NAT, מספקת לך רשת מאובטחת יותר, מפני שהכתובות של הרשת הפרטית שלך נסתרות לחלוטין מהאינטרנט. המחשב אשר משתף את החיבור, זה המשתמש ב-NAT, מבצע את כל התרגום של כתובות אינטרנט עבור הרשת הפרטית שלך, ולהיפך. אבל, שים לב שלמחשב ה-NAT אין את האפשרות לטפל בכל עומס הפניות לתרגום. דבר זה נובע מכך שיישומים מסוימים משתמשים בכתובות IP גם בשדות אחרים, מלבד שדות הכותרת של TCP/IP.

הפרוטוקולים הבאים אינם עובדים עם NAT:

- Kerberos
- IPSec (Internet Protocol Security Protocol)

פונקציונליות ההקצאה של DHCP ב-NAT מאפשרת לכל לקוחות DHCP ברשת להשיג ממחשב ה-NAT, באופן אוטומטי, כתובות IP, Subnet Mask, Default Gateway וכתובת שרת DNS. אם יש ברשת מחשב כלשהו שאינו מוגדר כלקוח DHCP, יהיה עליך להגדיר את הגדרות כתובות ה-IP באופן ידני.

כדי לחסוך עלויות בהקמת רשת קטנה נדרש רק שרת Windows 2000 אחד. שרת יחיד זה יכול לספק את כל שירותי NAT, APIPA (**A**utomatic **P**rivate **IP A**ddressing), ניתוב וגישה מרחוק (Routing and Remote Access) ו-DHCP.

כתובות פרטיות וציבוריות

אם רשת האינטראנט שלך אינה מחוברת לאינטרנט, תוכל להשתמש בכל מיעון IP שתחפוץ. אם דרוש לך חיבור ישיר (מנותב) או עקיף (דרך שרת Proxy או NAT) לאינטרנט, תוכל להשתמש בשני סוגי כתובות: כתובות ציבוריות וכתובות פרטיות.

כתובות ציבוריות

כתובות ציבוריות (Public Addresses) מוקצות על ידי מרכז המידע של רשת האינטרנט (InterNIC, **Inter**net **N**etwork **I**nformation **C**enter) ומורכבות ממזהי רשת מבוססי מחלקות (Class-based Network IDs) או מבלוקים של כתובות המבוססות על ניתוב תוך-תחומי חסר-מחלקות (CIDR, **C**lassless **I**nter-**D**omain **R**outing), הנקראות גם בלוקי CIDR. כתובות אלו מובטח שתהיינה ייחודיות בעולם האינטרנט. כאשר מוקצית כתובת ציבורית, מתוכנתים לנתבי האינטרנט נתיבים (Routes), כך שתעבורה לכתובת המוקצית תוכל להגיע ליעדה. תעבורה לכתובות יעד ציבוריות נגישה באינטרנט.

כתובות פרטיות

כל רכיב IP (IP Node) דורש שתהיה לו כתובת IP אשר היא ייחודית בכל אגד רשתות ה-IP (IP Internetwork). כאשר מדובר ברשת האינטרנט, כל צומת IP ברשת המחוברת לאינטרנט חייב שתהיה לו כתובת IP אשר היא ייחודית לכל רשת האינטרנט. ככל שרשת האינטרנט גדלה, ארגונים המתחברים לאינטרנט דרשו כתובת ציבורית עבור כל צומת באינטראנט שלהם. דרישה זו הציבה ביקוש אדיר למאגר הכתובות הציבוריות הזמינות.

כאשר ניתחו את צרכי הארגונים, שמו מפתחי האינטרנט לב לכך שבארגונים רבים לא נדרש חיבור ישיר בין רוב צמתי האינטראנט בארגון למארחי האינטרנט. מארחים אלה, שלא דרשו ערכת שירותי אינטרנט מסוימים, כגון גישה לרשת ה-Web (החלק הגרפי של רשת האינטרנט) ודואר אלקטרוני, ניגשו בדרך כלל לשירותי האינטרנט באמצעות יישומי שכבה שלישית (Third-Layer Applications), כגון שרתי Proxy ושרתי דואר. תוצאת הבדיקה היתה שלמרבית הארגונים דרוש מספר קטן בהרבה של כתובות ציבוריות עבור אותם צמתים (שרתי Proxy, נתבים, Firewalls ומתרגמים) אשר מחוברים באופן ישיר לאינטרנט.

בעבור המארחים שבתוך הארגון, ואשר אינם דורשים חיבור ישיר לאינטרנט, נדרשו כתובות IP שאינן מהוות כפילות של כתובות IP ציבוריות שכבר הוקצו. כדי לפתור בעיית מיעון זו, שמרו מפתחי האינטרנט חלק ממרחב כתובות ה-IP וקראו למרחב זה **מרחב הכתובות הפרטיות** (Private Addresses Space). כתובות IP פרטיות אינן מוקצות כמו כתובות ציבוריות. מכיון שמרחב הכתובות הציבורי אינו חופף למרחב הכתובות הפרטיות, כתובות פרטיות לעולם לא יהוו כפילות של כתובות ציבוריות. RFC 1918 מגדיר את טווחי הכתובות הפרטיות הבאים:

- **10.0.0.0 עד 10.255.255.255 .** רשת פרטית 10.0.0.0 היא רשת Class A המאפשרת את טווח כתובת ה-IP הבא: 10.0.0.1 ועד 10.255.255.254. לרשת פרטית 10.0.0.0 יש 24 סיביות מארח (24 Host bits) בהן ניתן להשתמש לסכמת רשת משנה כלשהי בארגון הפרטי.
- **172.16.0.0 ועד 172.31.255.255 .** רשת פרטית 172.16.0.0 יכולה להיחשב כבלוק של 16 מזהי רשת ממחלקה B (16 Class B Network IDs), או מרחב כתובות בן 20 סיביות הניתן לשיוך (20-bit Assignable Address Space) (20 סיביות מארח), אשר יכולה לשמש לכל סכמת רישות משנה (Subnetting) בארגון הפרטי. רשת פרטית 172.16.0.0 מאפשרת את טווח כתובת ה-IP הבא: 172.16.0.1 ועד 172.31.255.254.

❖ **192.168.0.0 ועד 192.168.255.255 .** רשת פרטית 192.168.0.0/16 יכולה להיחשב כבלוק של 256 מזהי רשת ממחלקה C (256 Class C Network IDs), או מרחב כתובות בן 16 סיביות הניתן לשיוך (16-bit Assignable Address Space) (16 סיביות מארח), אשר יכולה לשמש לכל סכמת רישות משנה (Subnetting) בארגון הפרטי. רשת פרטית 192.168.0.0 מאפשרת את טווח כתובת ה-IP הבא: 192.168.0.1 ועד 192.168.255.254.

כתובות פרטיות אינן נגישות מהאינטרנט. בשל כך, תעבורת אינטרנט אל מארח אשר יש לו כתובת פרטית חייבת להישלח באמצעות בקשות ליישומי שכבה שלישית (כגון שרת Proxy), להם יש כתובת ציבורית חוקית, או לחילופין, שהכתובת הפרטית שלו תתורגם לכתובת ציבורית חוקית באמצעות NAT (**N**etwork **A**ddress **T**ranslator), לפני שהיא נשלחת באינטרנט.

כיצד פועל NAT

מתרגם כתובות רשת הוא נתב IP, המוגדר במסמך RFC 1631, אשר יכול לתרגם את מספרי יציאות TCP/UDP של מנות כאשר הן מועברות בו. תאר לעצמך רשת משרדים קטנה ובה מספר מחשבים המחוברים לאינטרנט. בדרך כלל, יקבל המשרד כתובת ציבורית שהוקצתה לספק שירותי האינטרנט שלו עבור כל מחשב ברשת. אבל, כאשר מדובר ב-NAT, יכול העסק להשתמש במיעון פרטי (Private Addressing, כפי שמתואר במסמך RFC 1597) ולאפשר ל-NAT למפות את הכתובות הפרטיות שלו לכתובת IP ציבורית יחידה, או מספר מצומצם יותר של כתובות ציבוריות, כפי שמוקצה לו על ידי ספק השירותים. לדוגמה, אם עסק המשתמש ברשת פרטית 10.0.0.0 עבור האינטראנט שלו וקיבל מספק שירותי האינטרנט את הקצאת הכתובת הציבורית 198.200.200.1, ימפה ה-NAT (תוך שימוש במיפוי סטטי או דינמי) את כל כתובות ה-IP הפרטיות בהן נעשה שימוש ברשת 10.0.0.0 לכתובת ה-IP הציבורית 198.200.200.1.

מיפוי כתובות סטטי או דינמי

NAT יכול להשתמש במיפוי סטטי או דינמי. מיפוי סטטי (Static Mapping) מוגדר כך שהתעבורה עוברת תמיד במסלול מסוים. תוכל למפות את כל התעבורה אל ומאת מיקום מסוים ברשת הפרטית למיקום אינטרנטי מסוים. למשל, כדי להגדיר שרת אינטרנט במחשב ברשת הפרטית שלך, אתה יוצר מיפוי סטטי אשר ממפה את [Public IP Address, TCP Port 80] אל [Private IP Address, TCP Port 80].

מיפויים דינמיים נוצרים כאשר משתמשים ברשת הפרטית יוזמים תעבורה עם מיקומים באינטרנט. שירות NAT מוסיף באופן אוטומטי את המיפויים הללו לטבלת המיפוי שלו ומרענן את המיפויים בכל פעם שנעשה בהם שימוש. מיפויים דינמיים אשר אינם מרועננים מוסרים מטבלת המיפויים של NAT לאחר פרק זמן מוגדר. עבור חיבורי TCP, פרק זמן ברירת המחדל הוא 24 שעות. עבור תעבורת UDP, פרק זמן ברירת המחדל הוא דקה אחת.

תרגום נכון של שדות כותרת

כברירת מחדל מתרגם NAT כתובות IP ויציאות TCP/UDP. שינויים אלה לצרור נתוני IP (IP Datagram) דורשים שינויים וחישובים מחדש של השדות הבאים בכותרות IP, TCP ו- UDP :

- ❖ כתובת IP של המקור (Source IP Address)
- ❖ סכום ביקורת (Checksum) של TCP, UDP ו- IP
- ❖ יציאת מקור (Source Port)

אם כתובת ה-IP ונתוני היציאה קיימים רק בכותרות IP ו- TCP/UDP (לדוגמה, בתעבורת HyperText Transfer Protocol או World Wide Web) יכול פרוטוקול היישום להיות מתורגם באופן שקוף למשתמש. אבל, קיימים יישומים ופרוטוקולים אשר נושאים נתוני מיעון IP או יציאות (IP or Port Addressing) בתוך הכותרות שלהם. פרוטוקול FTP, לדוגמה, מאחסן את הייצוג הדצימלי מופרד-הנקודות של כתובות IP בכותרת FTP עבור פקודת היציאה של FTP (FTP Port Command). אם NAT אינו מתרגם כהלכה את כתובת ה-IP יתרחשו תקלות חיבוריות. מעבר לכך, במקרה של FTP, מכיון שכתובת IP מאוחסנת במבנה דצימלי מופרד-נקודות (Dotted-Decimal), יכולה כתובת ה-IP שבכותרת FTP להיות בגודל שונה. בשל כך, חייב NAT לשנות גם את מספרי הרצף של TCP, כדי להבטיח שלא יאבד מידע כלשהו.

עורכי NAT

במקרה בו רכיב NAT חייב בנוסף גם לתרגם ולהתאים את העומס שמעבר לכותרות IP, TCP ו-UDP, יש צורך בעורך NAT, NAT Editor. עורך NAT הוא רכיב בר-התקנה אשר יכול לשנות נכון את העומס שבדרכים אחרות לא היה מתורגם, כדי שניתן יהיה להעביר אותו דרך NAT. Windows 2000 כוללת עורכי NAT מובנים עבור הפרוטוקולים הבאים :

- ❖ FTP
- ❖ ICMP (Internet Control Message Protocol)
- ❖ PPTP (Point-to-Point Tunneling Protocol)
- ❖ NetBIOS Over TCP/IP

בנוסף, פרוטוקול הניתוב של NAT כולל תכנת Proxy עבור הפרוטוקולים הבאים :

- ❖ H.323
- ❖ Direct Play
- ❖ רישום -

Lightweight Directory Access Protocol (LDAP)-based Internet Locator Service (ILS)

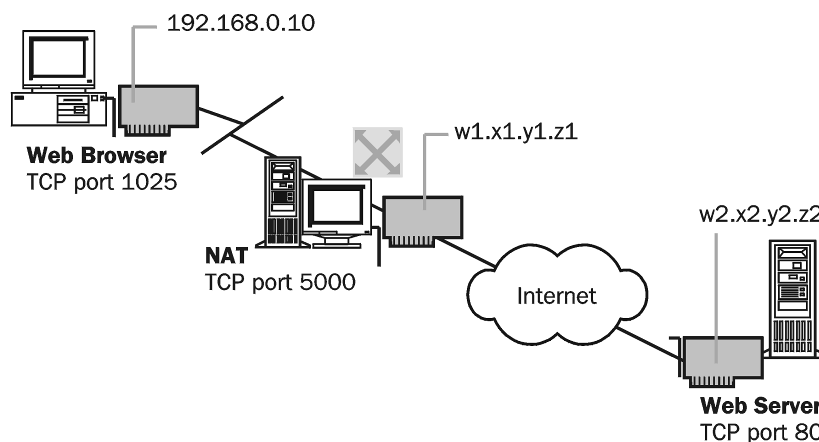
- ❖ Remote Procedure Call

הערה תעבורת IPSec אינה ניתנת לתרגום.

דוגמה ל-NAT

אם עסק קטן משתמש במזהה הרשת הפרטית 198.162.0.0 לשימוש האינטראנט שלו, וספק שירותי האינטרנט שלו הקצה עבורו את הכתובת הציבורית w1.x1.y1.z1, אז ה-NAT ממפה את כל הכתובות שברשת 198.162.0.0 אל כתובת ה-IP הציבורית w1.x1.y1.z1. אם מספר כתובות פרטיות ממופות לכתובת ציבורית יחידה, משתמש NAT ביציאות TCP ו-UDP הנבחרות באופן דינמי, כדי להבדיל בין מיקום אינטראנט אחד למשנהו. תרשים 12.1 מציג דוגמה לשימוש ב-NAT כדי לחבר את האינטראנט לרשת האינטרנט באופן שקוף למשתמש.

הערה השימוש ב- w1.x1.y1.z1 וב- w2.x2.y2.z2 נועד לייצג כתובות IP ציבוריות חוקיות, כפי שהן מוקצות על ידי InterNIC או ספק שירותי האינטרנט.



תרשים 12.1 שימוש ב-NAT כדי לחבר את רשת האינטראנט הפרטית לרשת האינטרנט הציבורית באופן שקוף למשתמש

תהליכי NAT ב- Routing and Remote Access של Windows 2000

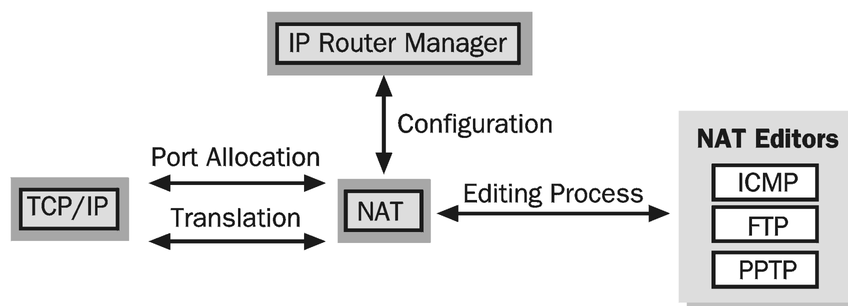
עבור Routing and Remote Access של Windows 2000, רכיב NAT יכול להיות מופעל על ידי הוספת NAT כפרוטוקול ניתוב ב-Snap-In של Routing and Remote Access.

הערה שירותי NAT זמינים גם באמצעות התכונה Internet Connection Sharing הזמינה בתיקיה Network and Dial-Up Connections, כפי שמוסבר בשיעור 2. Internet Connection Sharing מבצע את אותה הפעולה כמו פרוטוקול הניתוב NAT ב- Routing and Remote Access, אלא שהוא מוגבל מאוד בנוגע להגדרותיו. למידע אודות אופן הגדרת Internet Connection Sharing, ומתי עליך להעדיף את השימוש בו על פני השימוש בפרוטוקול הניתוב NAT של Routing and Remote Access, פנה למערכת העזרה של Windows 2000 Server.

יחד עם פרוטוקול הניתוב מותקנים גם מספר עורכי NAT. ‏NAT מתייעץ בעורכים כאשר מטענה של מנה מסוימת המתורגמת על ידו תואם לאחד מהעורכים המותקנים. העורכים משנים את המטען ומחזירים את התוצאה לרכיב NAT. ל-NAT יש אינטראקציה עם פרוטוקול TCP/IP בשתי דרכים חשובות:

- ❖ כדי לתמוך במיפוי יציאות דינמי, מבקש רכיב NAT מספרי יציאות TCP ו-UDP ייחודיים ממחסנית פרוטוקול TCP/IP, כאשר הדבר נדרש.
- ❖ עם TCP/IP, כדי שהמנות הנשלחות בין הרשת הפרטית והאינטרנט מועברות תחילה לרכיב NAT, לשם תרגומן.

תרשים 12.2 מציג את רכיבי NAT ואת יחסיהם ל-TCP/IP ולרכיבי נתב אחרים.



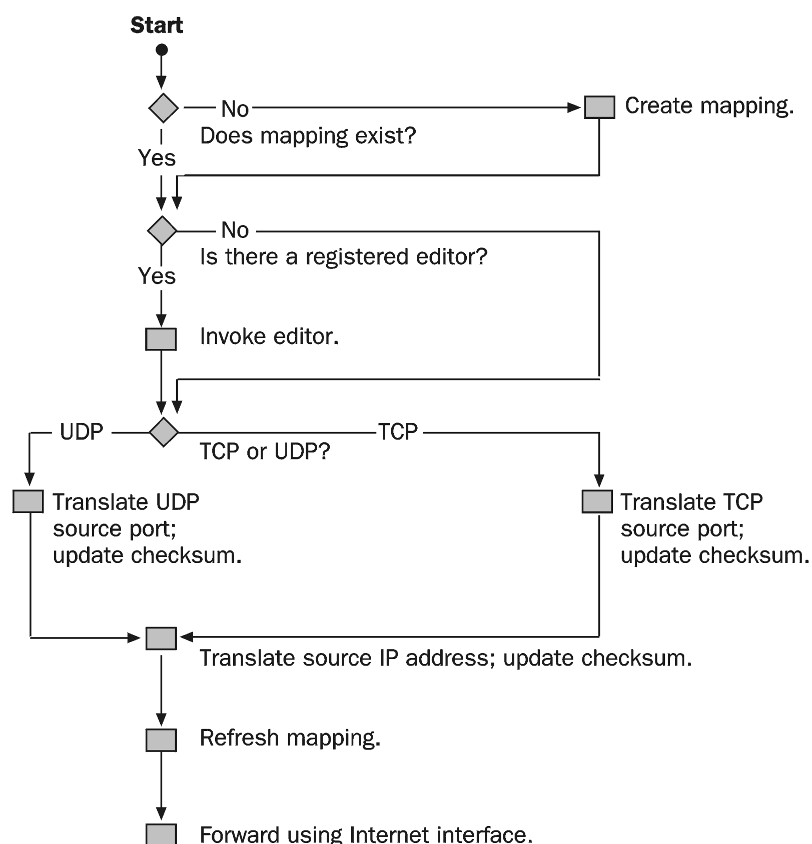
תרשים 12.2 רכיבי NAT

תעבורת אינטרנט יוצאת

עבור תעבורה מהרשת הפרטית אשר יוצאת (Outbound) לכיוון ממשק האינטרנט, NAT מעריך תחילה אם קיים עבור המנה, או שלא קיים, מיפוי כתובת/יציאה (סטטי או דינמי). אם לא, נוצר מיפוי דינמי. ה-NAT יוצר מיפוי בהתבסס על השאלה האם זמינה כתובת ציבורית אחת או יותר.

- ❖ אם רק כתובת ציבורית אחת זמינה, מבקש ה-NAT מספר יציאה TCP או UDP ייחודי עבור הכתובת הציבורית ומשתמש בה כיציאה הממופה.
- ❖ אם יש יותר מכתובת אחת זמינה, מבצע ה-NAT מיפוי כתובת-IP-פרטית - לכתובת-IP-ציבורית. לצורך מיפויים אלה, היציאות אינן מתורגמות. כאשר נדרשת הכתובת הציבורית האחרונה, עובר NAT לביצוע מיפוי כתובת-ליציאה, כפי שמתבצע הדבר במקרה של כתובת ציבורית יחידה.

לאחר המיפוי, מנסה NAT לאתר עורכים מתאימים ומפעיל אחד, אם יש צורך בכך. לאחר העריכה, משנה NAT את כותרות ה-IP ו- TCP או UDP ומעביר את המנה באמצעות ממשק האינטרנט. תרשים 12.3 מציג את NAT המעבד תעבורה היוצאת לכיוון האינטרנט.



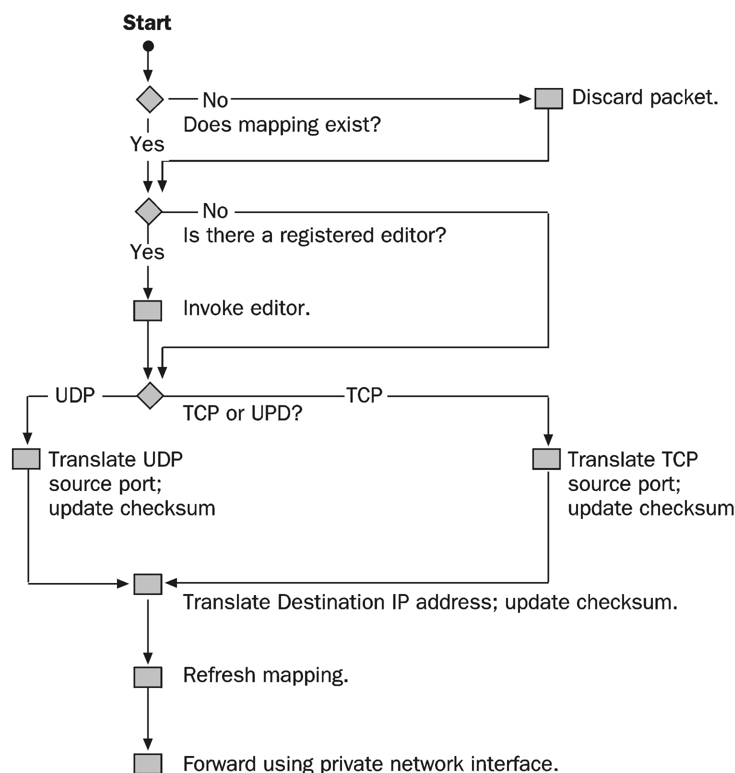
תרשים 12.3 NAT מעבד תעבורה היוצאת לכיוון האינטרנט

תעבורת אינטרנט נכנסת

עבור תעבורה מהרשת הפרטית אשר נכנסת ממשק האינטרנט, ה-NAT מעריך תחילה אם קיים עבור המנה, או שלא קיים, מיפוי כתובת/יציאה (סטטי או דינמי). אם לא קיים מיפוי עבור המנה, NAT מעלים אותה בשקט.

התנהגות זו מגינה על הרשת הפרטית ממשתמשים "לא נחמדים" מכיוון רשת האינטרנט. הדרך היחידה בה תעבורת אינטרנט מועברת לרשת הפרטית היא או כתגובה לתעבורה יזומה על ידי משתמש הרשת הפרטית אשר יצרה מיפוי דינמי, או מפני שקיים מיפוי סטטי כדי שמשתמשי האינטרנט יוכלו לגשת למשאבים מסוימים ברשת הפרטית.

לאחר המיפוי מנסה NAT לאתר עורכים מתאימים ומפעיל אחד, אם יש צורך בכך. לאחר העריכה משנה NAT את כותרות ה-IP ו- TCP או UDP ומעביר את המסגרת לממשק הרשת הפרטית. תרשים 12.4 מציג את NAT המעבד תעבורה הנכנסת מהאינטרנט.



תרשים 12.4 NAT מעבד תעבורה הנכנסת מהאינטרנט

רכיבים נוספים של פרוטוקול הניתוב NAT

כדי לפשט את תהליך הגדרת החיבור לאינטרנט של רשתות קטנות כולל פרוטוקול הניתוב NAT של Windows 2000 גם DHCP Allocator (מקצה DHCP) ו- DNS Proxy.

DHCP Allocator

רכיב ה- DHCP Allocator מספק נתוני תצורת כתובת IP למחשבים אחרים ברשת. DHCP Allocator הוא שרת DHCP בזעיר אנפין אשר מקצה כתובת IP, Subnet Mask, Default Gateway ואת כתובת ה-IP של שרת ה-DNS. עליך להגדיר מחשבים ברשת DHCP כלקוחות DHCP, כדי שיוכלו לקבל את נתוני התצורה באופן אוטומטי. כברירת מחדל, מחשבי Windows 2000, Windows NT, Windows 95 ו- Windows 98 מוגדרים כלקוחות DHCP.

טבלה 12.1 מציגה את אפשרויות ה-DHCP שבהודעות DHCPOFFER ו- DHCPACK המופקות על ידי ה- DHCP Allocator בעת תהליך חכירת DHCP. אין אפשרות לשנות אפשרויות אלו או להגדיר אפשרויות DHCP נוספות.

טבלה 12.1 אפשרויות תצורה של חכירת DHCP

מספר אפשרות	ערך אפשרות	תיאור
1	255.255.0.0	Subnet Mask
3	כתובת IP או ממשק פרטי	נתב (Default Gateway)
6	כתובת IP או ממשק פרטי	שרת DNS (מופק רק במידה והאפשרות DNS Proxy פעילה)
58 (0x3A)	5 דקות	זמן החידוש
59 (0x3B)	5 ימים	זמן איגוד מחדש
51	7 ימים	משך חכירת כתובת ה-IP
58 (0x0F)	domain name עיקרי של מחשב NAT	DNS domain

ה- DHCP Allocator תומך רק במרחב כתובות IP אחד, כפי שמוגדר בכרטיסיה Address Assignment שבתיבת דו-שיח Properties Of The Network Address Translation (NAT) Routing Protocol של יישום ה-Snap-In בשם Routing and Remote Access. ה-DHCP Allocator אינו תומך במספר מרחבים (Multiple Scopes), מרחבי-על (Superscopes) או מרחבי שידור לרבים (Multicast Scopes). אם דרושה לך פונקציונליות זו, עליך להתקין שרת DHCP ולבטל את רכיב ה- DHCP Allocator בפרוטוקול הניתוב NAT.

DNS Proxy

רכיב DNS Proxy פועל כשרת DNS עבור המחשבים ברשת שלך. שאילתות DNS הנשלחות על ידי מחשב NAT מועברות לשרת ה-DNS. תגובות לשאילתות DNS המתקבלות דרך שרת ה-NAT נשלחות שוב למחשב ברשת הביתית או המשרדית.

סיכום שיעור

NAT מאפשר לכתובות IP פרטיות להיות מתורגמות לכתובות IP ציבוריות, כדי שיוכלו לעבור אל ומאת האינטרנט. בדרך זו ניתן לאבטח את הרשת הפנימית מהאינטרנט, ויחד עם זאת לחסוך בעלויות הכרוכות באחזקת ובתחזוקת טווח כתובות ציבוריות. בדרך כלל, עסק קטן יקבל מספק שירותי האינטרנט שלו הקצאה לכתובת IP ציבורית, ממאגר הכתובות של הספק, עבור כל מחשב ברשת שלו. אבל, באמצעות NAT, יכול העסק הקטן להשתמש במיעון פרטי ולתת ל-NAT לבצע מיפוי של הכתובות הפרטיות לכתובת IP ציבורית אחת או יותר, כפי שהוקצו לו על ידי ספק שירותי האינטרנט.

שיעור 2: התקנת
Internet Connection Sharing

שיתוף התקשרויות לאינטרנט (ICS, **I**nternet **C**onnection **S**haring) היא תכונה של Network and Dial-Up Connections המאפשרת לך להשתמש ב- Windows 2000 כדי לחבר את הרשת המשרדית או הביתית שלך לאינטרנט. לדוגמה, ייתכן שאתה מעוניין לחבר את הרשת הביתית שלך לאינטרנט באמצעות חיבור בחיוג. בשיעור זה תלמד כיצד להתקין את ICS ב- Windows 2000.

לאחר שיעור זה, תוכל

- לאפשר את התכונה ICS ב- Windows 2000.
- להגדיר אפשרויות אינטרנט עבור ICS.

זמן לימוד משוער: 35 דקות

Internet Connection Sharing

שיתוף התקשרויות לאינטרנט (ICS, **I**nternet **C**onnection **S**haring) היא חבילה פשוטה הכוללת DHCP, NAT ו-DNS. תוכל להשתמש ב-ICS כדי לחבר בקלות את כל הרשת שלך לאינטרנט. מכיון ש-ICS מספק חיבור מתורגם, יכולים כל המחשבים ברשת לגשת למשאבי אינטרנט, כגון דואר אלקטרוני, אתרי אינטרנט ואתרי FTP. ICS מספק את היכולות הבאות:

- ❖ קלות הגדרה
- ❖ כתובת IP ציבורית יחידה
- ❖ טווח כתובות קבוע עבור מארחים
- ❖ DNS Proxy לשם הסדרת שמות
- ❖ מיעון IP אוטומטי

ICS מספק מיגוון רחב בהרבה של תכונות, חוץ מאשר תרגום כתובות. Microsoft הוסיפה תכונות רבות, כדי להפוך את הגדרת החיבור לאינטרנט פשוטה עד כמה שניתן. את ICS ניתן להגדיר ולנהל במלואו באמצעות Routing and Remote Access Manager. עבור רשת ביתית פשוטה, ניתן גם להפעיל אשף (Connection Sharing Wizard). האשף אינו מאפשר הגדרה של אילו מבין האפשרויות, אך יכול לאפשר לרשת ביתית להיות מחוברת לאינטרנט תוך מספר דקות. מה שמפשט את ההגדרה זה המיעון האוטומטי (Automatic Addressing) והסדרת שמות אוטומטית (Automatic Name Resolution) המתבצעים באמצעות רכיבי DNS Proxy, DHCP Allocator ו- WIN Proxy. כל אחד מאלו מספק תצורה מצומצמת של הגרסאות המלאות של שרתי DHCP, DNS ו-WINS.

על ידי אפשור ICS במחשב בו נעשה שימוש בחיבור לאינטרנט אתה מספק שירותי NAT, מיעון והסדרת שמות לכל המחשבים ברשת הביתית שלך. לאחר ש-ICS מאופשר והמשתמשים מוודאים את חיבורי הרשת שלהם ואת החיבוריות לאינטרנט, יכולים המשתמשים ברשת הקטנה (ביתית או משרדית) להשתמש ביישומים כגון

Internet Explorer או Outlook Express ממש כאילו היו מחוברים ישירות לספק השירות. מחשב ה-ICS מחייג לספק השירותים ויוצר חיבוריות, כדי שהמשתמשים האחרים יוכלו להגיע לכתובת או למשאבי האינטרנט הרצויים. כדי להשתמש בתכונה ICS, צריכים המשתמשים ברשת הקטנה שלך להגדיר את TCP/IP שב- Local Area Connection כך שיקבלו כתובת IP באופן אוטומטי.

אפשור Internet Connection Sharing

לפני שתאפשר את ICS במחשבי הרשת, שקול את הנקודות הבאות :

- ❖ אל תשתמש ב-ICS ברשת בה מוגדרים DCs אחרים של Windows 2000, שרתי DNS, Gateways, שרתי DHCP או מערכות בהן מוגדרת כתובת IP סטטית.
- ❖ כאשר אתה מאפשר את ICS, מקבל כרטיס הרשת המחובר לרשת הביתית/משרדית הקטנה הגדרות חדשות עבור כתובת ה-IP. חיבורי TCP/IP קיימים במחשב ICS אובדים, ויש צורך להקים אותם מחדש.
- ❖ כדי להשתמש בתכונה ICS, חייבים משתמשים ברשת הביתית/משרדית שלך להגדיר את TCP/IP שב- Local Area Connection לקבלת כתובת IP באופן אוטומטי.
- ❖ אם מחשב ה-ICS מחובר לאינטרנט באמצעות קו ISDN או מודם אנלוגי רגיל, עליך לוודא שתיבת הסימון Enable On-Demand Dial מסומנת.

➢ כדי לאפשר ICS בחיבור רשת

1. לחץ Start, הצבע על Settings, ובחר Network and Dial-Up Connections.
2. לחץ לחיצה ימנית על החיבור אותו אתה מעוניין לשתף (חיוג, VPN וכדומה), ומתפריט הקיצור בחר Properties.
3. בכרטיסיה Sharing סמן את תיבת הסימון Enable Internet Connection Sharing For This Connection.
4. אם אתה מעוניין שחיבור זה יחוייג באופן אוטומטי כאשר מחשב אחר ברשת מנסה לגשת למשאב אינטרנטי, סמן את תיבת הסימון Enable On-Demand Dial.

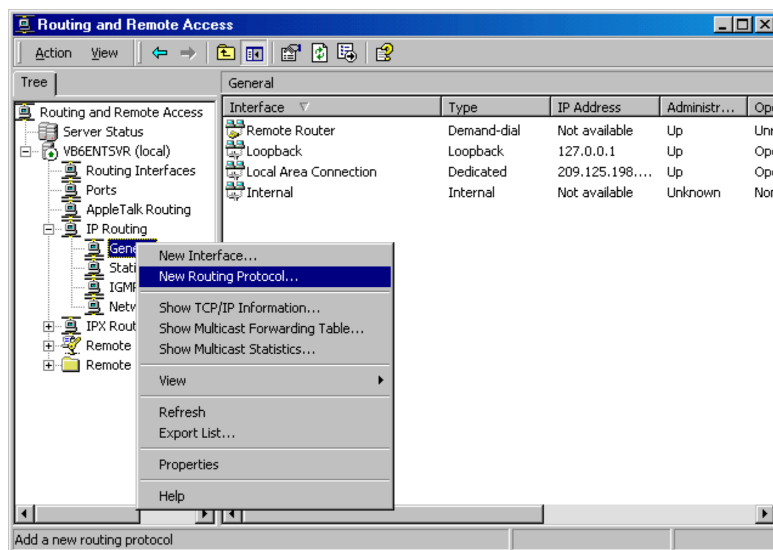
התקנת Internet Connection Sharing

הגדרת שיתוף התקשרויות מתבצעת באמצעות Routing and Remote Access Manager.

➢ כדי להתקין את Internet Connection Sharing

1. בחלון Routing and Remote Access Manager, פתח את התיקיה IP Routing, ולחץ לחיצה ימנית על General.
2. בחר New Routing Protocol, כפי שמוצג בתרשים 12.5.

   מופיעה תיבת דו-שיח Select Routing Protocol.
3. בתיבת דו-שיח Select Routing Protocol לחץ על Connection Sharing.



תרשים 12.5 Routing and Remote Access Manager

הגדרת אפשרויות האינטרנט לשיתוף התקשרויות אינטרנט

אם לא יצרת בעבר חיבור לאינטרנט השלם את הצעדים הבאים:

➤ כדי להקים חיבור לאינטרנט

1. פתח את Internet Explorer.
2. בחר את לחצן האפשרויות I want to set up my internet connection manually או את I want to connect through a Local Area Network (LAN), ולחץ Next.
3. לחץ על I connect through a Local Area Network (LAN), ולחץ Next.
4. נקה את תיבת הסימון Automatic discovery of proxy server [recommended], ולחץ Next.
5. אם אתה מעוניין להגדיר את חשבון הדואר האלקטרוני כעת, ואתה יודע את נתוני ההתחברות, לחץ Yes וספק את נתוני חשבון האינטרנט המתבקשים על ידי האשף. אם אינך מעוניין להגדיר את חשבון הדואר האלקטרוני כעת לחץ No, לחץ Next, ולחץ Finish.

אם יצרת בעבר חיבור לאינטרנט, תתבקש להשלים את הצעדים הבאים.

➤ כדי להגדיר את אפשרויות האינטרנט עבור ICS

1. פתח את תפריט Tools, ובחר Internet Options.
2. בכרטיסיה Connections לחץ על לחצן האפשרויות Never dial a connection, ולחץ על LAN Settings.

3. בתיבה Automatic Configuration בטל את הסימון ליד Automatically detect settings וליד Use automatic configuration script.

4. בתיבה Proxy server בטל את הסימון ליד Use a proxy server.

Internet Connection Sharing ו-NAT

כדי לחבר רשת משרדית/ביתית לאינטרנט תוכל להשתמש בחיבור מנותב (Routed) או בחיבור מתורגם (Translated). עבור חיבור מנותב, משמש המחשב בו פועלת מערכת ההפעלה Windows 2000 Server כנתב IP המעביר מנות בין הרשת הפנימית לבין האינטרנט הציבורית. למרות שעקרון העבודה פשוט יותר, חיבור מנותב דורש ידע מעמיק במיעון IP ובניתוב. אבל, תעבורה מנותבת מאפשרת מעבר של כל תעבורת IP בין מארחי הרשת הפנימית לאינטרנט. למידע נוסף, פנה למערכת העזרה המקוונת, בנושא Small Office/Home Office (SOHO) Network.

כאשר מדובר בחיבורים מתורגמים, משמש המחשב בו פועלת מערכת ההפעלה Windows 2000 Server כמתרגם כתובות רשת (מחשב NAT). ליצירת חיבורים מתורגמים במחשבים הפועלים בסביבת Windows 2000 Server יש צורך בפחות ידע בנושא מיעון IP וניתוב, והם מאפשרים הגדרת תצורה פשוטה של מארחים ושל נתב Windows 2000. אבל, ייתכן שלא כל תעבורת ה-IP תאופשר בין מארחי SOHO לבין מארחי האינטרנט.

ב- Windows 2000 Server תוכל להגדיר חיבור מתורגם לאינטרנט על ידי שימוש ברכיב ICS של Network and Dial-Up Connection או באמצעות פרוטוקול הניתוב NAT המסופק עם Routing and Remote Access. הן ICS והן NAT מספקים שירותי תרגום, מיעון והסדרת שמות למארחי SOHO.

כפי שתואר בסעיף הקודם, ICS מיועד לספק הגדרה בלחיצה בודדה (תיבת סימון אחת) במחשב בו פועלת מערכת ההפעלה Windows 2000, כדי לספק חיבור מתורגם לאינטרנט עבור כל המארחים ברשת. אבל, לאחר שאופשר, ICS אינו מאפשר הגדרה נוספת מעבר להגדרת היישומים והשירותים. לדוגמה, ICS מתוכנן להשיג כתובת IP יחידה מספק השירות (ISP) ואינו מאפשר לך לשנות את טווח כתובות ה-IP המוקצות למארחים.

כפי שלמדת בשיעור 1, פרוטוקול הניתוב NAT מיועד לספק את הגמישות המירבית בהגדרת מחשב Windows 2000 Server כך שיספק חיבור מתורגם לאינטרנט. NAT דורש צעדי הגדרה נוספים; אבל, ניתן להתאים באופן אישי כל צעד הגדרה. פרוטוקול NAT מאפשר קבלת טווח כתובות מספק השירות והגדרת טווח הכתובות המוקצה למארחים.

טבלה 12.2 מסכמת את התכונות והאפשרויות של ICS ושל NAT.

טבלה 12.2 תכונות NAT ו- ICS

ICS	NAT
הגדרה של תיבת סימון אחת	הגדרה ידנית
כתובת IP ציבורית יחידה	מספר כתובות IP ציבוריות
טווח כתובות קבוע עבור המארחים פנימיים	טווח כתובות הניתן להגדרה עבור המארחים הפנימיים
ממשק פנימי יחיד	מספר ממשקים פנימיים

ICS ו-NAT הן תכונות של Windows 2000 Server אשר נועדו לחבר רשתות SOHO לאינטרנט. ICS ו-NAT לא נועדו לשם:

- ❖ חיבור ישיר של רשתות פרטיות בינן לבין עצמן.
- ❖ חיבור רשתות בתוך אינטראנט.
- ❖ חיבור ישיר של רשתות בסניפים לרשת הארגונית.
- ❖ חיבור ישיר של רשתות בסניפים לרשת הארגונית באמצעות האינטרנט.

איתור וטיפול בתקלות בשיתוף קישוריות לאינטרנט (NAT)

תוכל לענות על השאלות הבאות כדי לאתר ולפתור תקלות הקשורות בשיתוף התקשרויות:

- ❖ **האם כל הממשקים שלך (פנימיים או חיצוניים) נוספו לפרוטוקול הניתוב Connection Sharing (NAT)?** עליך להוסיף הן את הממשק הציבורי (אינטרנט) והן את הממשק הפנימי (רשת ביתית/משרדית) לפרוטוקול הניתוב Connection Sharing (NAT).
- ❖ **האם התרגום מאופשר בממשק החיצוני (אינטרנט)?** עליך לוודא שהממשק של נתב Windows אשר מתחבר לאינטרנט מוגדר לתרגום. יש לבחור באפשרות Enable Translation Accross This Interface בכרטיסיה General של תיבת דו-שיח Properties Of Internet Interface.
- ❖ **האם שיתוף ההתקשרויות Connection Sharing מאופשר בממשק הפרטי (פנימי)?** עליך לוודא שהממשק בנתב Windows המחובר לרשת הפנימית מוגדר לשיתוף התקשרויות. יש לבחור באפשרות Allow Clients On This Interface To Access Any Shared Networks בכרטיסיה General של תיבת דו-שיח Properties Of The Home Interface.
- ❖ **האם מאופשר תרגום יציאת TCP/UDP?** אם יש ברשותך רק כתובת IP ציבורית יחידה, עליך לוודא שנבחרה האפשרות Translate TCP/UDP Headers בכרטיסיה General של תיבת דו-שיח Properties Of The External Interface.

- **האם טווח הכתובות הציבוריות שלך מוגדר כהלכה?** אם יש ברשותך מספר כתובות ציבוריות, עליך לוודא שהן הוקלדו כהלכה בכרטיסיה Address Pool של תיבת דו-שיח Properties Of Internet Interface. אם מאגר הכתובות שלך כולל כתובת IP שלא הוקצתה לך על ידי ספק השירות, אז תעבורת אינטרנט הממופה לאותה כתובת IP עשויה להיות מנותבת על ידי ספק השירות למיקום אחר.
- **האם הפרוטוקול בו משתמשת התוכנה ניתן לתרגום?** אם יש לך מספר תוכניות אשר נראה כאילו הן אינן עובדות עם NAT, תוכל לנסות ולהפעיל אותן ממחשב ה-NAT. אם הן עובדות ממחשב NAT ולא ממחשב ברשת הפרטית, ייתכן שתוכן המנות שיוצרת התוכנה אינו ניתן לתרגום (Not Translatable). תוכל לבדוק את הפרוטוקול בו משתמשת התוכנה ולהשוות זאת עם רשימת עורכי NAT הנתמכים.
- **האם אפשרות המיעון של Connection Sharing ברשת הביתית/משרדית פעילה?** אם לא הוגדרו ברשת הפרטית כתובת IP סטטיות, ודא שהאפשרות למיעון שיתוף ההתקשרויות (Connection Sharing Addressing) פעילה בממשק הרשת הפרטית. כדי לוודא זאת, לחץ על Interfaces בכרטיסיה Addressing שבתיבת דו-שיח Properties Of The Connection Sharing Object.

סיכום שיעור

ICS היא תכונה של Network and Dial-Up Connection המאפשרת לך להשתמש ב- Windows 2000 כדי לחבר את הרשת הביתית/משרדית שלך לאינטרנט. את ICS ניתן להגדיר ולנהל במלואה מתוך Routing and Remote Access Manager. על ידי אפשור ICS במחשב המשתמש בהתחברות בחיוג (Dial-up Connection) אתה מספק לכל מחשבי הרשת שלך שירותי NAT, מיעון (Addressing) והסדרת שמות (Name Resolution).

שיעור 3: התקנת והגדרת NAT

הכוונה העיקרית ב-NAT היא לחסוך במרחב כתובת ה-IP. יתרון נוסף של NAT הוא באספקת חיבוריות לאינטרנט ללא צורך להבין את נושא ניתוב IP או פרוטוקולי ניתוב IP. ניתן להשתמש ב-NAT ללא כל ידע או שיתוף פעולה כלשהו מצד ספק שירותי האינטרנט (ISP). התקשרות לספק השירות לצורך הוספת הקצאת ניתובים סטטיים אינה נדרשת. בשיעור זה תלמד כיצד להתקין ולהגדיר את NAT.

לאחר שיעור זה, תוכל

- לתאר חלק מהנושאים בהם יש להתחשב בתכנון, לפני יישום NAT.
- לאפשר מיעון NAT (NAT Addressing).
- להגדיר טווחי כתובות IP לממשק.
- להגדיר יציאות (Ports) ייחודיות לממשק.
- להגדיר יישומי רשת של NAT.

זמן לימוד משוער: 20 דקות

שיקולים בתכנון NAT

שימוש נפוץ ל-NAT הוא חיבור לאינטרנט מרשת ביתית/משרדית. כדי למנוע בעיות קיימים מספר שיקולי תכנון הצריכים להילקח בחשבון לפני שתיישם את NAT. לדוגמה, בדרך כלל כאשר משתמשים ב-NAT משתמשים בכתובות פרטיות בחלק הפנימי של הרשת. כפי שתואר בשיעור 1, כתובות פרטיות נועדו לרשתות פנימיות, כלומר כאלה שאינן מחוברות ישירות לאינטרנט. מומלץ להשתמש בכתובות פרטיות, ולא לבחור בכתובות באופן אקראי, מה שימנע את הסיכוי לכפילות בהקצאת כתובת. מעבר לכך, עליך לשקול ניתוב (Routing) במקום שימוש ב-NAT, מפני שניתוב מהיר ויעיל יותר, ופרוטוקול IP נועד להיות מנותב. אבל, כדי ליישם ניתוב נדרשות כתובות IP תקניות וחוקיות, וידע רב ב-domain.

נושאי מיעון IP

עליך להשתמש בכתובת IP הבאות, מתוך מזהי הרשתות הפרטיות של InterNIC:

- 10.0.0.0 עם 255.0.0.0 Subnet Mask
- 172.16.0.0 עם 255.240.0.0 Subnet Mask
- 192.168.0.0 עם 255.255.0.0 Subnet Mask

כברירת מחדל, NAT משתמש במזהה הרשת הפרטית 192.168.0.0 עם מסכת רשת המשנה 255.255.255.0 עבור רשת פרטית.

אם אתה משתמש בכתובות IP ציבוריות ברשת, אשר לא הוקצו על ידי InterNIC או ספק השירותים שלך, ייתכן שאתה משתמש במזהה רשת IP (IP Network ID) של ארגון אחר ברשת האינטרנט. דבר זה מוכר כמיעון IP לא חוקי (Illegal IP Addressing) או מיעון IP חופף (Overlapping IP Addressing). אם תשתמש בכתובות IP ציבוריות חופפות, לא תוכל

לגשת למשאבי האינטרנט של הכתובות החופפות. לדוגמה, אם אתה משתמש בכתובת 1.0.0.0 ובמסכת רשת המשנה 255.0.0.0 לא תוכל להגיע למשאבי אינטרנט כלשהם השייכים לארגון המשתמש ברשת 1.0.0.0. תוכל גם להוציא (Exclude) כתובות IP מסוימות מהטווח המוגדר. כתובות שהוצאו אינן מוקצות למארחים ברשתות פרטיות.

➢ כדי להגדיר שרת NAT

1. התקן ואפשר את Routing and Remote Access.

   באשף ההתקנה של Routing and Remote Access בחר באפשרויות עבור ICS וכדי להגדיר נתב עם פרוטוקול הניתוב NAT. לאחר שהאשף מסיים את פעולתו, מושלמות כל ההגדרות עבור NAT. אינך צריך להשלים את צעדים 2 עד 8. אם כבר אפשרת את Routing and Remote Access, השלם את הצעדים 2 עד 8, כפי הנדרש.

2. הגדר את כתובת ה-IP של ממשק הרשת הביתית.
3. עבור כתובת ה-IP של מתאם הרשת המחובר לרשת הביתית, עליך להגדיר את ההגדרות הבאות:
   - כתובת IP : 192.168.0.1
   - 255.255.255.0 Subnet Mask
   - ללא Default Gateway

הערה כתובת ה-IP המוזכרת בשלב 3 של הליך זה מבוססת על טווח ברירת המחדל של רשת 192.168.0.0 עם מסכת רשת המשנה 255.255.255.0, אשר מוגדרת לרכיב המיעון של NAT. אם תשנה את טווח ברירת מחדל זה, עליך לשנות את כתובת ה-IP של הממשק הפרטי במחשב ה-NAT, כך שתהיה הכתובת הראשונה בטווח המוגדר החדש. ככלל, השימוש בכתובת ה-IP הראשונה בטווח היא פעולה מומלצת, אך אינה מהווה דרישה של רכיבי NAT.

---

4. אפשר ניתוב על יציאת החיוג שלך.

   אם החיבור שלך לאינטרנט הוא חיבור קבוע המופיע ב-Windows 2000 כממשק LAN (כגון DDS, T-Carrier, Frame Relay, ISDN קבוע או מודם כבלים), או אם אתה מחבר את המחשב בו פועלת מערכת ההפעלה Windows 2000 לנתב אחר קודם לחיבור לאינטרנט, וממשק ה-LAN מוגדר עם כתובת IP, Subnet Mask ו- Default Gateway, בין אם סטטי ובין אם באמצעות DHCP, דלג לצעד 6.

5. צור ממשק חיבור-על-פי-דרישה (Demand-Dial) לספק שירותי האינטרנט שלך.

   עליך ליצור ממשק חיבור-על-פי-דרישה המאפשר ניתוב IP והמשתמש בציוד החיוג שלך ובנתוני המשתמש, בהם אתה משתמש להתחברות לספק השירותים (ISP).

6. צור ניתוב ברירת מחדל סטטי (Default Static Route) המשתמש בממשק האינטרנט שלך.

   עבור ניתוב ברירת מחדל סטטי, עליך לבחור את ממשק החיבור-על-פי-דרישה (לחיבורים בחיוג) או בממשק ה-LAN (בחיבורים קבועים או כאלו בהם מתווך נתב) המשמש להתחברות לאינטרנט. כתובת היעד היא 0.0.0.0 ומסכת הרשת היא 0.0.0.0. עבור ממשק חיוג-על-פי-דרישה לא ניתן להגדיר את כתובת ה-IP של השער.

7. הוסף את פרוטוקול הניתוב NAT.

הוראות להוספת פרוטוקול הניתוב NAT מופיעות בהליך הבא.

8. הוסף את ממשק הרשת הביתית וממשק האינטרנט לפרוטוקול הניתוב NAT.

9. אפשר מיעון NAT והסדרת שמות.

➢ **כדי להוסיף את NAT כפרוטוקול הניתוב**

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ובחר Routing And Remote Access.

2. ב- MMC Tree, לחץ על General תחת Routing and Remote Access\Server Name\IP Routing.

3. לחץ לחיצה ימנית על General, ומתפריט הקיצור בחר New Routing Protocol.

4. בתיבת דו-שיח Select Routing Protocol לחץ על Network Address Translation, ולחץ OK.

➢ **כדי לאפשר מיעון NAT**

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ובחר Routing And Remote Access.

2. ב- MMC Tree לחץ על NAT.

3. לחץ לחיצה ימנית על NAT, ומתפריט הקיצור בחר Properties.

4. בכרטיסיה Address Assignment סמן את תיבת הסימון ליד Automatically Assign IP Addresses By Using DHCP.

5. אם הדבר נחוץ, בתיבה IP Address and Mask הגדר את טווח כתובות ה-IP אותן יש להקצות ללקוחות DHCP ברשת הפרטית.

6. אם הדבר נחוץ, לחץ על Exclude והגדר את הכתובות אותן יש להוציא מטווח ההקצאה ללקוחות DHCP לרשת הפרטית, ולחץ OK.

כתובת ציבורית אחת או מספר כתובות ציבוריות

אם אתה משתמש בכתובת ציבורית אחת המוקצה לך על ידי ספק שירותי האינטרנט, אין צורך בהגדרות נוספות לכתובת IP. אם אתה משתמש במספר כתובות ציבוריות המוקצות לך על ידי ספק שירותי האינטרנט שלך, עליך להגדיר לממשק NAT את טווח כתובות ה-IP הציבוריות. עבור טווח הכתובות שהוקצה לך על ידי ספק השירות עליך לקבוע אם ניתן לבטא את טווח הכתובות הציבוריות, על ידי שימוש בכתובת IP ומסכה (Mask).

אם קיבלת הקצאה של מספר כתובות בחזקת 2 (2, 4, 8, 16 וכן הלאה), תוכל לבטא את הטווח באמצעות כתובת IP יחידה ומסכה. לדוגמה, אם קיבלת את ארבע כתובות ה-IP: 200.100.100.212, 200.100.100.213, 200.100.100.214 ו- 200.100.100.215, תוכל לבטא את כל ארבע הכתובות כ- 200.100.100.212, עם מסכה 255.255.255.252. אם לא ניתן

לבטא את הכתובות שלך בכתובת IP ו- Subnet Mask, תוכל להקליד אותם כטווח או כסדרה של טווחים, על ידי ציון כתובת ההתחלה וכתובת הסיום.

➢ **כדי להגדיר טווחי כתובות לממשק**

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ובחר Routing And Remote Access.
2. ב- MMC Tree לחץ על NAT.
3. בחלונית הפרטים (הימנית) לחץ לחיצה ימנית על הממשק אותו אתה מעוניין להגדיר, ומתפריט הקיצור בחר Properties.
4. בכרטיסיה Address Pool לחץ על Add.

אם אתה משתמש בטווח כתובות הניתן לביטוי ככתובת IP עם מסכת משנה, הקלד בתיבה Start Address את כתובת ה-IP הראשונה, ואילו בתיבה Mask הקלד את מסכת רשת המשנה. אבל, אם אתה משתמש בטווח כתובות IP אשר אינן ניתנות לביטוי ככתובת IP עם מסכת משנה הקלד בתיבה Start Address את כתובת ה-IP הראשונה, ואילו בתיבה End Address הקלד את כתובת ה-IP האחרונה.

אפשור חיבורים נכנסים

שימוש רגיל ב-NAT עבור רשת ביתית/משרדים מאפשר חיבורים יוצאים (Outbound Connections) מהרשת הפרטית לרשת הציבורית. תוכניות כגון דפדפני אינטרנט הפועלות מתוך הרשת הפרטית יוצרים חיבורים למשאבי אינטרנט. התעבורה החוזרת מהאינטרנט עשויה לעבור דרך NAT, מפני שהחיבור נוצר מהרשת הפרטית. כדי לאפשר למשתמשי אינטרנט לגשת למשאבים ברשת הפרטית שלך עליך לעשות כך :

- הגדר כתובת IP סטטית בשרת המשאבים, כולל כתובת IP (מטווח כתובות ה-IP שמקצה מחשב ה-NAT), Subnet Mask (מטווח כתובות ה-IP שמקצה מחשב ה-NAT), Default Gateway (כתובת ה-IP הפרטית של מחשב ה-NAT) ושרת DNS (כתובת ה-IP הפרטית של מחשב ה-NAT).
- הוצא את כתובת ה-IP של שרת המשאבים מטווח כתובות ה-IP המוקצות על ידי מחשב ה-NAT.
- הגדר יציאה מיוחדת (Special Port). יציאה מיוחדת היא כתובת IP ומספר יציאה הממופים באופן סטטי לכתובת פרטית ומספר יציאה. יציאה מיוחדת ממפה חיבור פנימה (Inbound Connection) ממשתמש אינטרנט לכתובת מסוימת ברשת הפרטית שלך. על ידי השימוש ביציאות מיוחדות תוכל ליצור ברשת הפרטית שלך שרת אינטרנט, אשר יהיה נגיש מהאינטרנט.

➢ **כדי להגדיר לממשק יציאות מיוחדות**

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ובחר Routing and Remote Access.
2. בחלונית הפרטים לחץ לחיצה ימנית על הממשק אותו אתה מעוניין להגדיר, ומתפריט הקיצור בחר Properties.

3. בתיבה Protocols בכרטיסיה Special Ports, לחץ על UDP או על TCP, ולחץ על Add.
4. בתיבה Incoming Port הקלד את מספר היציאה של התעבורה הציבורית הנכנסת.
5. אם מוגדר טווח של כתובות ציבוריות, לחץ על On this address pool entry, ואז הקלד את כתובת ה-IP הציבורית של התעבורה הציבורית הנכנסת.
6. בתיבה Outgoing Port הקלד את מספר היציאה של משאב הרשת הפרטית.
7. בתיבה Private Address הקלד את הכתובת הפרטית של משאב הרשת הפרטית.

הגדרת יישומים ושירותים

ייתכן שתצטרך להגדיר יישומים ושירותים כך שיעבדו כראוי דרך האינטרנט. לדוגמה, אם משתמשים ברשת הביתית/משרדית שלך מעוניינים לשחק את המשחק Diablo עם משתמשים אחרים באינטרנט, NAT חייב להיות מוגדר עבור היישום Diablo.

➢ כדי להגדיר יישומי רשת NAT

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ובחר Routing and Remote Access.
2. ב- MMC Tree לחץ על NAT.
3. לחץ לחיצה ימנית על NAT, ומתפריט הקיצור בחר Properties.
4. בכרטיסיה Translation לחץ על Applications.
5. כדי להוסיף יישום רשת, לחץ על Add בתיבת דו-שיח Applications.
6. בתיבת דו-שיח Add Application, הקלד את ההגדרות עבור יישום הרשת, ולחץ OK.

הערה תוכל גם לערוך או להסיר יישומי רשת NAT קיימים על ידי לחיצה על Edit או Remove בתיבת דו-שיח Applications.

חיבורי VPN מרשת מתורגמת

כדי לגשת לרשת אינטראנט פרטית באמצעות חיבור VPN (**V**irtual **P**rivate **N**etwork) מרשת מתורגמת, תוכל להשתמש בפרוטוקול PPTP וליצור חיבור VPN ממארח ברשת הפרטית לשרת VPN ברשת אינטראנט פרטית שנייה. פרוטוקול הניתוב NAT כולל עורך NAT לתעבורת PPTP. חיבורי L2TP over IPSec (Layer 2 Tunneling Protocol over IPSec) אינם פועלים דרך שרת NAT.

רשתות פרטיות וירטואליות ו-NATs

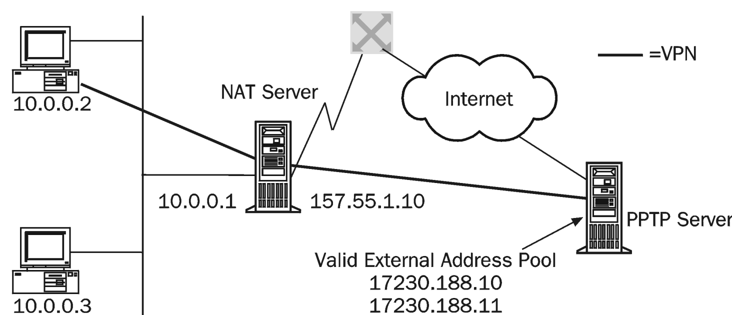
לא כל סוגי התעבורה ניתנים לתרגום על ידי NAT. חלק מהיישומים דורשים כתובות IP מוטבעות (Embedded IP Addresses, לא בכותרות IP, IP Headers), או שהם עשויים להיות מוצפנים. עבור יישומים כגון אלה, ניתן לתעל דרך NAT באמצעות PPTP. ל-PPTP דרוש עורך, אשר מוטמע כחלק מ-NAT. רק כותרות מסוג GRE (**G**eneric **R**outing **E**ncapsulation)

נערכות או מתורגמות. צרור נתוני ה-IP (IP Datagram) המקורי אינו מושפע. דבר זה מאפשר להצפנה, או ליישומים אחרים שאינם נתמכים, לעבור דרך NAT.

מקורן של מנות PPTP יתורגם לכתובת NAT. מנת ה-IP הסגורה (Encapulated) תקבל כתובת מקור המוקצית לה על ידי שרת PPTP. כאשר המנה עוברת את שרת ה-PPTP מוסרת ממנה הסגירה וכתובת המקור תהיה זו שהוקצתה על ידי שרת ה-PPTP. אם שרת ה-PPTP משתמש במאגר של כתובות אינטרנט חוקיות, ללקוח יש כרגע כתובת חוקית והוא יכול לגשת לכל מקום באינטרנט. בדרך זו כל יישום יעבוד, מכיון שצרור נתוני ה-IP המקורי אינו מתורגם. רק הסגירה (Encapsulation) או האריזה (Wrapper) מתורגמים על ידי NAT.

הערה L2TP **אינו** דורש עורך NAT. אבל, L2TP עם IPSec **אינו יכול להיות מתורגם על ידי** NAT. **לא יכול להיות עורך** NAT **עבור** IPSec.

שיטה זו של מעקף NAT יעילה רק כאשר קיים שרת PPTP אליו ניתן לתעל. הדבר יהיה יעיל עבור סניפים או משתמשים ביתיים המתעלים את דרכם לרשת ארגונית, כפי שמתואר בתרשים 12.6.



תרשים 12.6 יישום VPN דרך שרת NAT

סיכום שיעור

כאשר משתמשים ב-NAT, משתמשים בדרך כלל בכתובות פרטיות עבור הרשת הפנימית. מומלץ להשתמש בכתובות הפרטיות המוגדרות, במקום לבחור כתובות IP באופן אקראי, מפני שאלו האחרונות עלולות לגרום לכפילות כתובות, דבר שאינו מקובל באינטרנט. כדי למנוע בעיות, עליך לזהות את נושאי התכנון, קודם ליישום NAT. שימוש רגיל ב-NAT מרשת ביתית/משרדית מאפשר חיבורים יוצאים מהרשת הפרטית לרשת הציבורית. ייתכן שתצטרך להגדיר יישומים ושירותים כך שיעבדו כראוי דרך האינטרנט. בנוסף, זכור שלא כל תעבורת רשת ניתנת לתרגום על ידי NAT, מפני שיישומים אחדים עשויים לכלול כתובות IP מוטבעות, או שהם מוצפנים. עבור יישומים אלה תוכל לתעל דרך NAT תוך שימוש ב-PPTP.

שאלות סיכום

השאלות הבאות נועדו לחזק את הנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות על שאלה, עיין בשיעור המתאים ונסה את השאלה שנית. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואחר כך בעברית.

Answering the following questions will reinforce key information presented in this chapter. If you are unable to answer a question, review the appropriate lesson and then try the question again. Answers to the questions can be found in Appendix A, "Questions and Answers".

1. What is the purpose of NAT?
2. What are the components of NAT?
3. If a small business is using the 10.0.0.0 private network for its intranet and has been granted the public IP address of 198.200.200.1 by its ISP, to what public IP address does NAT map all private IP addresses being used on network 10.0.0.0?
4. What must you do to allow Internet users to access resources on your private network?

1. מהי מטרת NAT?
2. מהם רכיבי NAT?
3. אם עסק קטן משתמש ברשת פרטית 10.0.0.0 עבור רשת האינטראנט שלו, וספק שירותי האינטרנט שלו הקצה לו כתובת ה-IP הציבורית 198.200.200.1, לאיזו כתובת ציבורית ממפה NAT את כל הכתובות הפרטיות בהן נעשה שימוש ברשת הפרטית 10.0.0.0?
4. מה עליך לעשות כדי לאפשר למשתמשי אינטרנט גישה למשאבים ברשת הפרטית שלך?

פרק 13

יישום שירותי אישורים

אודות פרק זה

אישורים (Certificates) הם המרכיב הבסיסי של תשתית המפתח הציבורי של Microsoft (PKI, **P**ublic **K**ey **I**nfrastructure). אישורים מאפשרים למשתמשים להשתמש בכניסה למערכת באמצעות כרטיס חכם, לשלוח הודעות דואר אלקטרוני מוצפנות ולחתום על מסמכים אלקטרוניים. אישורים מונפקים, מנוהלים, מחודשים ומבוטלים על ידי רשות אישורים (Certificate Authority). בפרק זה תלמד כיצד להתקין ולהגדיר אישורים.

לפני שתתחיל

להשלמת פרק זה צריך שיהיה ברשותך:

- ❖ מחשב בו מותקנת מערכת ההפעלה Windows 2000 Server.
- ❖ Active Directory מותקן.
- ❖ DNS מותקן.

שיעור 1: הכרת אישורים

בשיעור זה תלמד אודות אישורים דיגיטליים ו- Certificate Services של Windows 2000. אישורים הם חלק חשוב מאוד של ה-PKI של Microsoft. בנוסף, תלמד אודות רשויות אישורים (CA, **C**ertificate **A**uthorities) הנתמכות על ידי Certificate Services של Windows 2000.

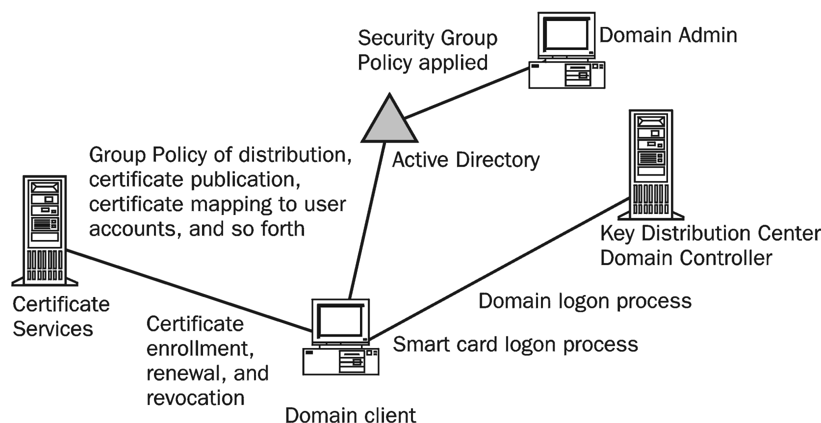
לאחר שיעור זה, תוכל

- להגדיר אישור.
- להסביר את מרכיבי האישור.
- לתאר את השימוש באישור.
- להסביר את ההבדלים שבין Cas ארגוניים ל- Cas עצמאיים.

זמן לימוד משוער: 25 דקות

סקירת אישורים

אישור (נקרא גם אישור דיגיטלי או מפתח ציבורי דיגיטלי) הוא מסמך דיגיטלי המאשר את איגוד המפתח הציבורי ליישות. המטרה העיקרית של אישור (Certificate) היא לתת את הביטחון שהמפתח הציבורי הנכלל באישור אכן שייך ליישות ששמה מופיע באישור. כפי שמוצג בתרשים 13.1, האישור משחק תפקיד מרכזי ב-PKI של Microsoft.



תרשים 13.1 שירותי Certificate המשולבים ב- Active Directory ושירותי אבטחה מבוזרים

אישור יכול לכלול מפתח ציבורי אשר נחתם על ידי יישות נסמכת (Trusted Entity). אבל, המבנה והתחביר בהם נעשה שימוש נרחב ביותר עבור אישורים דיגיטליים מוגדר על ידי ITU (**I**nternational **T**elecommunications **U**nion), האיגוד הבינלאומי לטלקומוניקציה), במסמך ITU-T Recommendation X.509. תרשים 13.2 מציג אישור אשר יכול לשמש לאימות השולח של הודעת דואר אלקטרוני.



תרשים 13.2 אישור לדוגמה

אישור X.509 מכיל מידע המזהה את המשתמש, כמו גם מידע אודות הרשות שהפיקה את האישור, כולל מספר סידורי (Serial Number), תקופת תוקף האישור (Validity Period), שם המוציא לאור (Issuer Name), חתימת המוציא לאור (Issuer Signature) ושם הנושא (או המשתמש). הנושא (Subject) יכול להיות אדם פרטי, עסק, בית ספר או ארגון אחר, כולל CA (**C**ertificate **A**uthority).

כיצד יוצרים אישור

אישורים (Certificates) מונפקים על ידי רשויות אישורים (CA). רשות אישורים יכולה להיות שירות או יישות נסמכים המוכנים לערוב ולאמת את זהותם של אלה להם היא מנפיקה אישורים, ואת שיוכם למפתחות מסוימים. חברות עשויות להנפיק אישורים עבור העובדים בהן, בתי ספר ינפיקו אישורים ללומדים בהם וכדומה. ברור ומובן מאליו שהמפתח הציבורי של רשות אישורים חייב להיות אמין (ומקובל ככזה), אחרת האישורים שיונפקו על ידי אותה רשות לא ייחשבו לאמינים. מכיון שכל אחד יכול לקרוא לעצמו רשות אישורים (CA), רצוי לזכור שאישורים הם אמינים בדיוק כפי שהחברה מחזיקת המפתח הציבורי (מנפיקת האישור) אמינה. ששת הצעדים הבאים מתארים את התהליך של בקשה והנפקה של אישור.

1. **יצירת צמד מפתחות.** המועמד מחולל צמד מפתחות (פרטי וציבורי), או שמופק עבורו צמד שכזה על ידי רשות כלשהי בארגון שלו.
2. **איסוף המידע הנדרש.** המועמד אוסף את המידע אותו רשות האישורים דורשת לשם הנפקת האישור. מידע זה יכול לכלול את כתובת הדואר האלקטרוני של המועמד, תעודת לידה, טביעות אצבע, מסמכים נוטריוניים - כל מה שרשות האישורים צריכה כדי להיות בטוחה שהמועמד הוא מי שהוא טוען שהוא. רשויות מאשרות, להן דרישות הזדהות מחמירות במיוחד, מנפיקות אישורים בעלי אמינות רבה - זאת אומרת שהאישורים המונפקים על ידיהן נחשבים לאמינים במיוחד. לרשויות מאשרות עצמן יש רמת אמינות גבוהה, בינונית או נמוכה.

3. **בקשת האישור.** המועמד שולח את הבקשה לקבלת אישור, אשר מכילה את המפתח הציבורי שלו ומידע נדרש אחר, לרשות האישורים. הבקשה לאישור עשויה להיות מוצפנת באמצעות המפתח הציבורי של רשות האישורים. בקשות רבות מתבצעות באמצעות דואר אלקטרוני, אך ניתן גם לשלוח אותן באמצעות דואר רגיל או שירותי שליחויות, למשל כאשר הבקשה עצמה חייבת לקבל אישור נוטריוני.
4. **אימות נתונים.** רשות האישורים מחילה את חוקי המדיניות הנהוגים אצלה כדי לוודא שהמועמד יקבל את האישור המיוחל. כפי שהדבר בעת אימות זהות, מדיניות האימות והתהליכים הדרושים משפיעים על משך הזמן שיקח לרשות האישורים להפיק את האישור שלה.
5. **יצירת האישור.** רשות האישורים יוצרת וחותמת על מסמך דיגיטלי המכיל את המפתח הציבורי של המועמד ומידע נדרש אחר. החתימה של רשות האישורים מאמתת את איגוד שם נושא האישור למפתח הציבורי של נושא האישור. מסמך חתום זה הוא האישור.
6. **שליחת האישור.** רשות האישורים שולחת את האישור למועמד, או שהיא מפרסמת אותו ישירות במדריך המיועד לכך, על פי הצורך.

כיצד משתמשים באישור

אישורים משמשים להפגנת אמינות חוקיותם של מפתחות ציבוריים מסוימים. אישור חייב להיות חתום באמצעות המפתח הפרטי של מפיק האישור; אחרת, זה אינו אישור. בשל כך, חתימת מנפיק האישור יכולה להיבדק תוך שימוש במפתח הציבורי שלו. אם יישות כלשהי סומכת על אמינותו של המנפיק, אז אותה יישות יכולה לסמוך גם על כך שהמפתח הציבורי הנכלל באישור שייך לנושא הרשום באישור.

רשות אישור ארגונית ועצמאית

Sertificate Services כוללים שני מודולי מדיניות המאפשרים שתי מחלקות של רשויות אישורים (CAs): רשות אישור ארגונית (Enterprise CA) ורשות אישור עצמאית (Standalone CA). בתוך שתי מחלקות אלו, יכולים להיות שני סוגים של CA: CA שורש (Root CA) ו-CA כפופה (Subordinate CA). מודולי המדיניות מגדירים את הפעולות אותן יכולה CA לבצע כאשר היא מקבלת בקשה להנפקת אישור, והם ניתנים לשינוי על פי הצורך.

CAs מאורגנות בדרך כלל במבנה היררכי בו הרשות האמינה ביותר נמצאת בראש. ה-PKI של Windows 2000 מקבל מודל היררכי של CA. ייתכן שיהיו בו מספר מבנים היררכיים שאינם קשורים זה בזה; אין כל חובה שכל ה- CAs יישתפו הורה ברמה העליונה.

רשות אישור ארגונית

בארגון, ה-CA שורש (Root CA) הארגונית היא בעלת האמינות הגבוהה ביותר. ב-Windows 2000 domain יכולה להיות יותר מאשר CA שורש אחת, אך יכולה להיות רק CA שורש ארגונית (Enterprise Root CA) אחת בכל היררכיה נתונה. כל ה- CAs האחרות בהיררכיה הן CA ארגוניות כפופות (Enterprise Subordinate CA).

ארגון אמור להתקין CA ארגונית אם הוא מתעתד להנפיק אישורים למשתמשים ומחשבים בתוך הארגון פנימה. אין צורך להתקין CA בכל תחום בארגון. לדוגמה, משתמשים ב-Child Domain יכולים להשתמש ב-CA של Parent Domain. ל-CA ארגוניות יש מודול מדיניות מיוחד האוכף את האופן בו אישורים מעובדים ומונפקים. מידע המדיניות המשמש מודולים אלה נשמר באופן מרוכז ב- Active Directory של Windows 2000.

הערה Active Directory **ושירות** DNS **חייבים לפעול במחשב קודם להתקנת** CA **ארגונית.**

רשות אישור עצמאית

ארגון אשר מתעתד להנפיק אישורים למשתמשים ולמחשבים מחוץ לארגון חייב להתקין CA עצמאית (Stand-Alone CA). ניתן שתהיינה מספר CA עצמאיות, אך יכולה להיות רק CA עצמאית אחת בכל היררכיה. כל ה-CAs האחרות חייבות להיות CA עצמאיות כפופות או CA ארגוניות כפופות.

ל- CA עצמאית יש מודול מדיניות פשוט יחסית, אשר אינו מאחסן מידע כלשהו באופן מרוחק. בשל כך, CA עצמאית אינה זקוקה לנוכחותו של שירות Active Directory של Windows 2000.

סוגי CA

דרישות ההתקנה של ארבעה סוגי ה-CA הזמינות מתוך Certificate Services, כפי שמתואר בסעיפים הבאים.

CA שורש ארגונית (Enterprise Root CA)

CA שורש ארגונית היא שורש ההיררכיה של ה-CA הארגונית. ארגון צריך להתקין ולהגדיר CA שורש ארגונית במידה והוא מתעתד להנפיק אישורים למשתמשים ולמחשבים בתוך הארגון. בארגונים גדולים, ה-CA השורש הארגונית משמשת רק כדי להנפיק אישורים ל-CA ארגוניות כפופות. ה-CA הארגוניות הכפופות מנפיקות את האישורים למשתמשים ולמחשבים. CA שורש ארגונית דורשת:

- שירות DNS של Windows 2000
- שירות Active Directory של Windows 2000
- הרשאות מנהלתיות (Administrative Privileges) בכל השרתים

CA ארגונית כפופה (Enterprise Subordinate CA)

CA ארגונית כפופה היא ה-CA המנפיקה את האישורים בתוך הארגון, אך היא אינה בעלת האמינות הגבוהה ביותר בארגון; היא כפופה ל-CA אחרת בהיררכיה.

ל-CA ארגונית כפופה יש את הדרישות הבאות:

- היא חייבת להיות משויכת ל-CA אשר תעבד את הבקשות לאישורים המגיעות מה-CA הכפופה. זו יכולה להיות CA מסחרית או CA עצמאית.
- שירות DNS של Windows 2000
- שירות Active Directory של Windows 2000
- הרשאות מנהלתיות (Administrative Privileges) בכל השרתים

CA שורש עצמאית (Stand-Alone Root CA)

CA שורש עצמאים היא שורש היררכיית האמינות של ה-CA. CA שורש עצמאית דורשת הרשאות מנהלתיות בשרת המקומי. ארגון צריך להתקין ולהגדיר CA שורש עצמאית במידה וה-CA תנפיק אישורים מחוץ לרשת הארגונית, ועליה להיות ה-CA שורש. בדרך כלל, CA שורש מנפיקה אישורים רק ל-CAs כפופות לה.

CA עצמאית כפופה (Stand-Alone Subordinate CA)

CA עצמאית כפופה היא CA הפועלת כשרת אישורים בודד, או שהיא קיימת בהיררכיית אמינות של CA. על ארגון להתקין ולהגדיר CA עצמאית כפופה כאשר היא תנפיק אישורים ליישויות מחוץ לארגון.

ל-CA עצמאית כפופה יש את הדרישות הבאות:

- היא חייבת להיות משויכת ל-CA אשר תעבד את הבקשות לאישורים המגיעות מה-CA הכפופה. זו יכולה להיות CA מסחרית חיצונית.
- הרשאות מנהלתיות (Administrative Privileges) בכל השרתים.
- הרשמת אישורים (Certificate Enrollmant) הוא התהליך להשגת אישור דיגיטלי.

סיכום שיעור

בשיעור זה למדת שאישורים הם מרכיב יסודי של ה-PKI של Microsoft. אישורים מאפשרים למשתמשים להשתמש בכניסה למערכת באמצעות כרטיס חכם, לשלוח הודעות דואר אלקטרוני מוצפנות, לחתום על מסמכים דיגיטליים וכיוצא בזה. אישורים מונפקים, מנוהלים, מחודשים ומבוטלים על ידי CAs. בנוסף, למדת בשיעור זה גם כיצד להתקין ולהגדיר אישורים.

שיעור 2: התקנה והגדרה של רשות אישורים

בשיעור זה תסקור את האישורים בפירוט רב יותר, על ידי כך שתלמד כיצד להתקין ולהגן על ה-CA שלך. אחר כך, יוצג בפניך התהליך של הרשמת אישורים (Certificate Enrollment) והדרכים השונות לעשות זאת.

לאחר שיעור זה, תוכל

- להסביר כיצד להתשמש ב- Certificate Authority Manager.
- להסביר כיצד להתקין CA.
- להסביר כיצד להגן על CA.
- לתאר את תהליך הרשמת האישור.

זמן לימוד משוער: 35 דקות

פריסת CA

בעת ביצוע התרגול הבא יותקנו גם CAs. את תהליך ההתקנה יבצע מנהל מערכת (System Administrator) ויוביל אותו Certificate Services Installation Wizard. סעיף זה יידון בנקודות מפתח בהן יש להתחשב לפני תחילת תהליך ההתקנה.

- ❖ **הקמת Windows 2000 domain**. אם הכוונה היא ליצור CA ארגונית, יש ליצור Domain קודם להתקנת Certificate Services.
- ❖ **שילוב ב- Active Directory.** מידע הקשור ל-CAs הארגוניות נכתב בזמן ההתקנה לאובייקט ה-CA שב- Active Directory. דבר זה מספק ללקוחות domain נתונים אודות CAs זמינות וסוג האישורים שהן מנפיקות.
- ❖ **בחירת השרת המארח.** CA שורש יכולה לפעול בכל פלטפורמת שרת של Windows 2000, כולל DC (**D**omain **C**ontroller). בעת הבחירה יש להתחשב בגורמים, כגון דרישות אבטחה פיסית, עומס צפוי ודרישות חיבוריות.
- ❖ **מתן שם.** שמות של CA מאוגדים לאישורים שלהן ולכן לא ניתן לשנותם. מעבר לכך, לא ניתן גם לשנות את שמו של המחשב בו פועלים השירותים Certificate Cervices. בעת החשיבה על שם ה-CA קח בחשבון גורמים, כגון מוסכמות מתן שמות בארגון ודרישות עתידיות להבדלה בין ה-CAs המנפיקות אישורים. שם ה-CA (או השם הנפוץ) הוא נושא חשוב ביותר, מפני שהוא משמש לזיהוי אובייקט ה-CA שנוצר ב- Active Directory עבור CA ארגונית.
- ❖ **יצירת מפתחות.** צמד המפתחות פרטי/ציבורי של ה-CA ייוצר (יחולל) בעת תהליך ההתקנה, והוא ייחודי ל-CA זו.
- ❖ **אישור CA.** עבור CA שורש, תהליך ההתקנה יחולל באופן אוטומטי אישור CA חתום באופן עצמי, תוך שימוש בצמד המפתחות פרטי/ציבורי. עבור CA צאצא (Child CA), תעמוד בפני מנהל המערכת האפשרות לחולל בקשה לאישור, אשר עשויה להיות מוגשת ל-CA שורש או מתווכת (Intermediate).

- **מדיניות הנפקה.** תוכנית ההתקנה של CA ארגונית תתקין ותגדיר באופן אוטומטי את מודול מדיניות ברירת המחדל עבור ה-CA. תוכנית ההתקנה של CA עצמאית תתקין ותגדיר באופן אוטומטי את מודול המדיניות העצמאית. אם יימצא הצורך, ניתן להחליף את מדיניות ברירת המחדל במדיניות מותאמת אישית (Custom).

לאחר שנוצרה CA שורש, ניתן להתקין CAs מתווכות או מנפיקות כפופות ל-CA שורש זו. ההבדל המשמעותי היחיד במדיניות ההתקנה טמון בכך שנוצרת בקשה לאישור (Certificate Request) אשר תוגש ל-CA שורש או CA מתווכת. בקשה זו ניתנת לניתוב באופן אוטומטי ל-CAs מקוונות המאותרות באמצעות Active Directory, או להיות מנותבות באופן ידני בתרחיש שאינו מקוון. בכל מקרה, התוצאה תהיה אישור אותו יש להתקין ב-CA לפני שהיא תוכל להתחיל לבצע את תפקידה.

מודל האמון (Trust Model) של CA ארגונית עשוי או עשוי שלא להתאים למודל האמון של Windows 2000 domain לא נדרשת הקבלה ישירה בין יחסי האמון (Trust Relationships) שבין CAs למול יחסי האמון שבין ה-domains. אין דבר המונע מ-CA בודדת מלתת שירותים ליישויות ממספר domains, ואפילו ליישויות מחוץ לגבולות ה-domain. בדומה, ל-domain נתון יכולות להיות מספר CAs ארגוניות.

אבטחת CA

CAs הן משאבים בעלי ערך רב, ובדרך כלל רצוי לספק להן רמה גבוהה של אבטחה. פעולות מסוימות אשר רצוי להתייחס אליהן כוללות:

- **הגנה פיסית.** מכיון ש-CAs מייצגות יישות בה ניתן אמון רב בתוך הארגון, יש להגן עליהן מפני נגישות של גורמים שאינם מורשים בכך. דרישה זו תלויה בערך הנרכש של האישורים המונפקים על ידי CA זו. בידוד פיסי של שרת CA במתקן בו הגישה אפשרית רק למנהלי האבטחה, יכול להקטין באופן דרמטי את הסיכון לפגיעה פיסית כלשהי.
- **ניהול מפתחות.** המפתח הפרטי של ה-CA מספק את הבסיס לאמון בתהליך האישור ויש להגן עליו מפני שינויו. מודולי חומרת הצפנה (הנגישים עבור Certificate Services באמצעות CryptoAPI CSP) יכולים לספק אחסון מוגן מפני שינויים עבור המפתח, ומבודדים את תהליך ההצפנה עצמו מהתוכנות האחרות הפועלות בשרת. דבר זה מקטין באופן משמעותי את הסיכוי שמפתח ה-CA ישוכפל.
- **שחזור.** אובדן CA - כתוצאה מכשל חמור בחומרה, למשל - יכול לגרום למספר בעיות ניהוליות ותפעוליות, ולמנוע ביטולם של אישורים קיימים. Certificate Services תומכים בגיבוי של מופע CA, כך שניתן לשחזר אותה במועד מאוחר יותר. זהו פרט חשוב מאין כמוהו בתהליך הכולל של ניהול CA.

הבהרה CSP, **C**ryptographic **S**ervice **P**rovider - ספק שירותי הצפנה. גוף האחראי על יצירה והריסה של מפתחות, ועל השימוש בהם למיגוון משימות הצפנה. חלק מגופים אלה מספק אלגוריתמי הצפנה חזקים יותר, ואת חלקם ניתן למצוא בכרטיסים חכמים. (צרל)

הרשמת אישור

תהליך קבלת אישור דיגיטלי נקרא הרשמת אישור (Certificate Enrollment). ה-PKI של Windows 2000 תומכת בהרשמת אישור עבור CA ארגונית, עצמאית או של צד-שלישי.

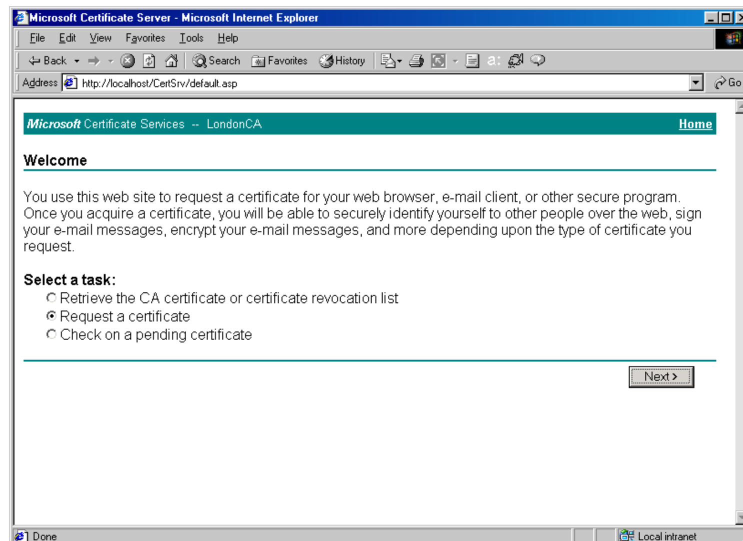
תמיכה בהרשמה מיושמת באופן של תעבורה בלתי-תלויה (Transport-Independent) ומבוססת על הודעות בקשה לאישור, העושות שימוש בתקנים תעשייתיים עבור מפתח קריפטוגרפי ציבורי (PKCS ,**P**ublic **K**ey **C**ryptography **S**tandards) מספר 10 (PKCS #10) ותגובות מספר 7 (PKCS #7), המכילות את תוצאת האישור או מחרוזת האישורים. בעת כתיבת שורות אלה, תומכים האישורים במפתחות ובחתימות RSA, מפתחות וחתימות DSA ומפתחות Diffie-Hellman.

שיטות להרשמה מרובה

PKI תומכת בשיטות להרשמה מרובה (Multiple Enrollment), כולל הרשמה מבוססת-אינטרנט, אשף הרשמה והרשמה אוטומטית מונחת-מדיניות, המתרחשת כחלק מתהליך כניסת המשתמש למערכת. בעתיד מתכוונת Microsoft לערב את תהליך הרשמת האישור באופן שיתאים לטיוטת CRS (**C**ertificate **R**equest **S**yntax) המונחת כיום על שולחנה של קבוצת העבודה PKIX, המהווה חלק מכוח המשימה של הנדסת האינטרנט (IETF ,**I**nternet **E**ngineering **T**ask **F**orce).

הרשמה מבוססת-אינטרנט

תהליך ההרשמה מבוססת האינטרנט (Web-Based Enrollment) מתחיל בבקשה אותה מגיש הלקוח לקבלת אישור, ומסתיים בהתקנת האישור ביישום הלקוח. Certificate Services כוללים גם בקרת הרשמה מבוססת HTTP עם טפסים, כפי שנראה בתרשים 13.3, עבור הרשמת אישורים מותאמת ואל דפים אלה ניגשים מתוך דף ההרשמה (Certificate Services Enrollment Page), אשר זמין מדף כלי ניהול האינטרנט של Certificate Services (http://<server_name>/certsrv/default.asp). תוכל להתאים באופן אישי את הדפים של כלי ניהול האינטרנט, כדי לשנות את האפשרויות העומדות בפני המשתמש או כדי לספק לו קישורים לעזרה מקוונת, תמיכה או הוראות למשתמש.



תרשים 13.3 הרשמת אישור באמצעות דפי אינטרנט

הרשמת אישור לקוח

Certificate Services תומכים בהרשמת אישור לקוח תוך שימוש ב- Internet Explorer גירסה 3 ואילך. כדי להשיג אישור באמצעות דפדפן זה, פותח הלקוח דף אימות (Authentication Page) ומגיש את מידע הזיהוי האישי שלו. לאחר ש- Certificate Services יוצרים עבורו את האישור הוא מוחזר לדפדפן, אשר מתקין את האישור בלקוח.

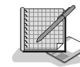
הרשמה אוטומטית

תהליך ההרשמה האוטומטית מבוקר על ידי שני מרכיבים עיקריים: סוגי האישורים (Certificate Types) ואובייקטים של הרשמה אוטומטית (Autoenrollment Objects). אלה משולבים עם אובייקט מדיניות קבוצתית ועשויים להיות מוגדרים על בסיס אתר (Site), Domain, יחידה ארגונית (OU, **O**rganizational **U**nit), מחשב (Computer) או משתמש (User).

סוגי אישורים מספקים תבנית עבור אישור ומשייכים אותו לשם נפוץ, לשם קלות הניהול. התבנית מגדירה מרכיבים כגון דרישות מתן השם, תקופת תוקף, CSPs מאושרים ליצירת מפתח פרטי, אלגוריתמים והרחבות אותן יש לכלול באישור. סוגי האישורים מחולקים באופן לוגי לאישורי מכונה ואישורי משתמש, ומוחלים על מדיניות האובייקטים בהתאם. לאחר שהוגדרו, זמינים אלה לשימוש עם אובייקטי ההרשמה האוטומטית ועם אשף ההרשמה (Certification Enrollment Wizard).

מנגנון זה אינו מחליף את מדיניות ההנפקה של ה-CA הארגונית, אלא משולב בו. שירות ה-CA מקבל קבוצה של סוגי אישורים כחלק מאובייקט המדיניות שלו. אלה משמשים את מודול מדיניות הארגון כדי להגדיר את סוגי האישורים שמותר ל-CA להנפיק. ה-CA דוחה בקשות לאישורים אשר אינן עומדות בקריטריונים אלה.

אובייקט ההרשמה האוטומטית מגדיר מדיניות עבור אישורים הצריכים להיות מוחזקים על ידי יישות ב-domain. דבר זה ניתן ליישם על בסיס מכונה או משתמש. סוגי האישורים משולבים על ידי ייחוסם לאובייקטי סוג האישור, ויכולים להיות כל סוג מוגדר. אובייקט ההרשמה האוטומטית מספק מידע מספק כדי לקבוע האם ליישות יש את האישור המבוקש, והוא רושם אישורים אלה ב-CA הארגונית במידה והם חסרים בה. אובייקטי ההרשמה האוטומטית גם מגדירים מדיניות לגבי חידוש האישור. דבר זה ניתן להגדרה על ידי מנהל מערכת (Administrator) כך שייתרחש קודם לפקיעת תוקפו של האישור, ותומך בפעולה לאורך זמן ללא צורך בהתערבות כלשהי מצד המשתמש. אובייקטי ההרשמה האוטומטית מעובדים, וכל המטלות הנדרשות מבוצעות, בכל פעם שהמדיניות מרועננת (בזמן הכניסה למערכת, אובייקט Group Policy מתרענן וכדומה).



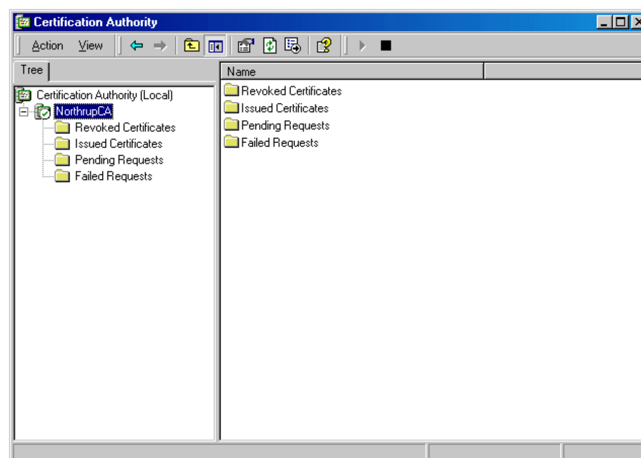
תרגול: התקנת CA עצמאית כפופה

➢ כדי להתקין CA עצמאית כפופה

1. בלוח הבקרה (Control Panel) לחץ לחיצה כפולה על Add/Remove Programs.
2. לחץ על Add/Remove Windows Components.
3. סמן את תיבת הסימון ליד Certificate Services, ולחץ Next.
4. בחר באפשרות Stand-alone Root CA, ולחץ Next.
5. מלא את פרטי הזיהוי של ה-CA.
6. בתיבה CA Name הקלד את הערך <ComputerName>CA, ולחץ Next.
7. השתמש במיקום בברירת המחדל לאחסון הנתונים, ולחץ Next.
8. בעת תהליך ההתקנה של ה-CA ייתכן שתצטרך ללחוץ על OK, כדי לעצור את השירות World Wide Web Publishing Service, ותצטרך לציין את המיקום בו שמורים קבצי ההתקנה של Windows 2000 (ובמיוחד הקבצים *.Certsrv).
9. לחץ Finish.
10. סגור את חלון Add/Remove Programs.

➢ כדי לבקש ולהתקין אישור מ-CA מקומית

1. הפעל את Certificate Authority Manager. שים לב שהשירות מופעל (סימן), כפי שניתן לראות בתרשים 13.4.



תרשים 13.4 Certificate Authority Manager

2. הפעל את Internet Explorer, והתחבר לכתובת:
http://<your_server>/certsrv/default.asp
3. בקש אישור עבור הדפדפן (Web Browser Certificate). הבקשה תלויה ועומדת (Pending).
4. סגור את Internet Explorer.

5. פתח את Certificate Authority ובחר בתיקיה Pending Requests. לחץ לחיצה ימנית על הבקשה שלך. בתפריט הקיצור הצבע על All Tasks, ובחר Issue.

   בחלונית השמאלית בחר בתיקיה Issued Certificates ושים לב שהבקשה שלך עובדה וכי הונפק בעבורה אישור.

6. הפעל את Internet Explorer, התחבר לכתובת:

http://<your_server>/certsrv/default.asp

   בחר באפשרות Pending Certificate Request, והתקן את האישור.

7. בחלון Internet Explorer פתח את תפריט Tools, לחץ על Internet Options, בחר בכרטיסיה Content, ולחץ על Certificates.

8. מרשימת האישורים בחר באישור שלך, ולחץ על View. שים לב שהאישור הונפק על ידי המחשב שלך, וסגור את כל החלונות.

אחסון מפתח הצפנה

בתוך תשתית המפתח הציבורי של Microsoft (ה-PKI) מאוחסנים ומנוהלים מפתחות ההצפנה והאישורים המשויכים להם, על ידי מערכת משנה הנקראת CryptoAPI. מפתחות מנוהלים על ידי CSPs, ואילו אישורים מנוהלים על ידי מחסן אישורי CryptoAPI (CryptoAPI Certificate Store). מחסני האישורים הם מאגרי אישורים, יחד עם מאפיינים משויכים. כמוסכמה, מגדיר PKI חמישה מחסני אישורים תקניים, ואלו מתוארים בטבלה 13.1.

טבלה 13.1 מחסני אישורים תקניים של PKI

מחסן	תיאור
MY	מחסן זה משמש לאחסון אישורי הלקוח או המחשב, שהמפתח הפרטי המשויך להם זמין.
CA	מחסן זה משמש לאחסון אישורים ש-CCA מנפיקה או מתווכת, כדי להשתמש בהם בעת בניית שרשראות אימות אישורים (Certificate Verification Chains).
TRUST	מחסן זה משמש לאחסנת אישורי רשימות אמון (Trust Lists). אלה הם מנגנונים חלופיים המאפשרים למנהל מערכת לציין אוסף של CAs אמינים. היתרון בהם הוא שהם חתומים באופן דיגיטלי ולכן ניתן לשדרם בקישורים שאינם מאובטחים.
ROOT	מחסן זה מחזיק רק אישורים החתומים באופן עצמי (Self-Signed) עבור CAs שורש אמינות.
UserDS	מחסן זה מספק תצוגה לוגית של מאגר האישורים המאוחסנים ב-Active Directory (לדוגמה, במאפיין userCertificate של האובייקט User). מטרתו היא לפשט את הגישה למאגרים חיצוניים אלה.

אלה הם מחסנים לוגיים אשר יכולים לייצג מבט כללי ועקבי של האישורים הזמינים, אשר יכולים להתקיים במספר מחסנים פיסיים (כונן קשיח, כרטיסים חכמים וכדומה). תוך שימוש בשירותים אלה יישומים יכולים לשתף אישורים, וכך הם מבטיחים פעולה עקבית תחת מדיניות מנהלתית. פונקציות ניהול האישורים תומכות בקידוד אישורי X.509 v3 ומספקות פונקציות מניה כדי לסייע באיתור אישור מסוים.

כדי לפשט את פיתוח היישומים, שומר המחסן MY מאפייני אישורים המציינים CSP ושם ערכת-מפתח (Key-Set) עבור מפתח פרטי משויך. לאחר שהיישום בחר את האישור בו ישתמש, הוא יכול להשתמש במידע זה כדי להשיג הקשר CSP (CSP Context) עבור המפתח הפרטי התואם.

חידוש אישור

חידוש אישור (Certificate Renewal) דומה במידת מה להרשמה, אך מנצל את יחסי האמון (Trust Relationships) המועברים בירושה מאישור קיים. חידוש יוצא מנקודת הנחה שהיישות המבקשת מבקשת אישור חדש עם אותן התכונות כמו אלו של אישור חוקי קיים, אבל עם אורך חיים ארוך יותר. חידוש עשוי להשתמש במפתח ציבורי קיים, או במפתח ציבורי חדש.

חידוש הוא יתרון בעיקר עבור ה-CA. בבקשת החידוש ניתן לטפל ביעילות רבה יותר, מפני שאין צורך לשוב ולוודא את תכונות האישור. כרגע נתמך חידוש האישור ב-Windows 2000 עבור אישורים שנרשמו באופן אוטומטי. לגבי מנגנונים אחרים, מטופל החידוש כמו בקשת הרשמה חדשה.

עדיין לא הוגדרו פרוטוקולי הודעות תקניים לצורך חידוש האישורים, אך אלו נכללים בטיוטת IETF PKIX CRS. לאחר שתקנים אלה יאושרו, מתכננת Microsoft ליישם את מבנה ההודעות המשויך.

התאוששות אישור ומפתח

לצמדי מפתחות ציבוריים ואישורים נוטים לייחס ערך גבוה. אם הם אובדים כתוצאה מכשל חמור במערכת, ייתכן שהחלפתם תארך זמן יקר ולגרימת נזק כספי. כדי לטפל באירוע כגון זה תומך ה-PKI של Windows 2000 באפשרות לגבות ולשחזר הן את האישורים והן את המפתחות המשויכים להם. פעולה זו ניתנת לביצוע באמצעות הכלים המנהלתיים לניהול האישורים.

כאשר מייצאים אישור באמצעות Certificate Manager, חייב המשתמש לציין האם יש לייצא גם את צמד המפתחות המשויך לאישור זה. אם אפשרות זו נבחרת, המידע מיוצא כהודעת PKCS #12 מוצפנת (בהתבסס על סיסמה אותה מספק הלקוח). בשלב מאוחר יותר ניתן יהיה לייבא הודעה זו למערכת, או למערכת אחרת, כדי לשחזר את האישור ואת המפתחות.

פעולה זו מניחה שצמד המפתחות ניתן לייצוא על ידי ה-CSP. דבר זה יהיה נכון עבור ה-CSPs הבסיסיים של Microsoft, במידה ודגלון הייצוא הוגדר בזמן יצירת המפתח. CSPs של צד-שלישי עשויים לתמוך או שלא לתמוך בייצוא מפתח פרטי. לדוגמה, CSPs של כרטיסים חכמים אינם תומכים בדרך כלל בפעולה כגון זו. בעבור CSPs של תוכנה, הכוללים מפתחות שאינם ניתנים לייצוא, האלטרנטיבה היא לשמור גיבוי מערכת מושלם, הכולל את כל נתוני הרישום.

נדידה

נדידה (Roaming) במובן של הדיון הנוכחי היא האפשרות להשתמש באותו יישום מבוסס מפתח ציבורי במחשבים שונים בסביבת Windows 2000 בארגון. הדרישה העיקרית היא

לגרום לכך שמפתחות הקריפטוגרפיה של המשתמשים והאישורים שלהם יהיו זמינים בכל רגע בו הם מתחברים. ה-PKI של Windows 2000 תומכת בכך בשתי דרכים.

ראשית, אם נעשה שימוש ב-CSPs מבוססי Microsoft, מפתחות ואישורים נודדים נתמכים על ידי מנגנון הפרופיל הנודד (Roaming Profile). לאחר שאופשר פרופיל נודד עבור המשתמש הופך הדבר לשקוף עבורו. לא מן הנמנע ש-CSPs של צד-שלילי לא יתמכו בנדידה, מפני שבדרך כלל הם משתמשים בשיטות שונות של שימור נתוני מפתח, בדרך כלל באמצעי חומרה.

התקני אסימון חומרה (Hardware Token Devices), כגון כרטיסים חכמים, תומכים בנדידה אם קיים בהם התקן לאחסון פנימי של האישור. ה-CSPs של כרטיסים חכמים המגיעים עם פלטפורמת Windows 2000 תומכים בפונקציונליות זו. תמיכה בנדידה מושגת על ידי העברת אסימון החומרה יחד עם המשתמש.

ביטול

לאישורים יש בדרך כלל אורך חיים ארוך. קיימות מספר סיבות לכך שאישורים אלה עשויים להפוך לבלתי אמינים קודם לפקיעתם. דוגמאות לכך הן:

- פגיעה, או חשד לפגיעה במפתח הפרטי
- זיוף בעת קבלת האישור
- שינוי מצב

פונקציונליות מבוססת-מפתח ציבורי יוצאת מנקודת הנחה שלצורך האימות המבוזר אין צורך בתקשורת ישירה עם יישות אמינה מרכזית, הערבה לפרטים שסופקו. עובדה זו יוצרת את הצורך לנתוני ביטול (Revocation) אותם ניתן להפיץ ליחידים המנסים לאמת אישורים.

הצורך בנתוני ביטול, והדייקנות הנדרשת לכך, תלויה ביישום. כדי לתמוך במיגוון תרחישים ביצועיים, מכליל ה-PKI של Windows 2000 תמיכה ברשימות ביטול אישורים תקניות (CRLs, **C**ertificate **R**evocation **L**ists). CAs ארגוניות תומכות בביטול אישורים בפרסום CRL ל- Active Directory באמצעים מנהלתיים. לקוחות domain יכולים לקבל מידע זה, לטמון (Cache) אותו באופן מקומי ולהשתמש בו כאשר הם מוודאים ומאמתים אישורים. אותו מנגנון בדיוק תומך ב-CRLs שפורסמו על ידי CA מסחריות, או על ידי מוצרי שרת אישורים (Certificate Server) של צד-שלישי, בתנאי שה-CRLs המפורסמים נגישים ללקוחות דרך הרשת.

אמון

אימות אישור (Certificate Verification) הוא בראש מעיני לקוחות המשתמשים ביישומים מבוססי מפתח ציבורי (PK-Based). אם אישור של יישות-קצה נתונה מופיע בשרשרת (Chain) של CA אמינה מוכרת, ואם השימוש האמור באישור תואם להקשר היישום, אז הוא ייחשב כחוקי. אם אחד מבין שני התנאים אינו מתמלא, ייחשב האישור כחסר תוקף.

בתוך ה-PKI, עשויים משתמשים לקבל החלטות לגבי אמון, אשר ישפיעו על עצמם בלבד. הם עושים זאת על ידי התקנת או מחיקת CAs שורש נסמכות ועל ידי הגדרת מגבלות שימוש משויכות. כל זאת מתבצע על ידי שימוש בכלי ניהול האישורים. בתוך הארגון,

אמור הדבר להוות את היוצא מהכלל, ולא את כללי הארגון. ניתן להניח שיחסי אמון אלה יתהוו כחלק ממדיניות הארגון. יחסי אמון הנוצרים על ידי מדיניות מופצים (Propagate) באופן אוטומטי למחשבי לקוח של Windows 2000.

שורשי CA אמינים

האמון ב-CAs שורש עשוי להיקבע על ידי מדיניות כך שייצור יחסי אמון המשמשים את לקוחות ה-domain בעת אימות אישורי PK (מפתח ציבורי). קבוצת ה-CAs האמינות מוגדרת באמצעות עורך המדיניות הקבוצתית, Group Policy Editor. ניתן להגדיר אותה על בסיס מחשב ואז היא תיושם לכל המשתמשים במחשב זה.

בנוסף לקביעת CA שורש כאמינה, יכול מנהל המערכת לקבוע מאפייני שימוש המשויכים ל-CA. אם הדבר מוגדר, יוגבלו המטרות שלשמן תקפים האישורים המונפקים על ידי ה-CA. הגבלות מוגדרות בהתאם למזהי אובייקט (Object Identifier) כפי שמוגדר עבור ההרחבה ExtendedKeyUsage בטיוטה הראשונה של IETF PKIX חלק 1. נכון להיום, אלה מספקים דרכים להגבלת השימוש לכל אחד מהשילובים הבאים:

- אימות שרת
- אימות לקוח
- חתימת קוד
- דואר אלקטרוני
- מערכת קצה של IPSec
- תעלת IPSec
- משתמש IPSec
- חתימת זמן
- מערכת קבצים מוצפנת (Microsoft **E**ncrypted **F**ile **S**ystem ,EFS)

סיכום שיעור

בשיעור זה למדת כיצד להתקין ולהגן על ה-CA שלך. CAs הן משאבים רבי חשיבות, וחשוב להקפיד להגן עליהן. בנוסף למדת כיצד לספק הרשמה של אישורים, ואת הדרכים המגוונות לבצע זאת. כדי להשיג אישור לקוח, על הלקוח לפתוח דף אימות ולספק נתונים מזהים. אחר כך יוצר Certificate Services את האישור עבור הלקוח, אשר מוחזר לדפדפן ומותקן בלקוח.

שיעור 3: ניהול אישורים

לאחר שתתחיל להנפיק אישורים, או שלקוחות יבקשו שתנפיק עבורם אישורים, ניהול אותם אישורים הופך לנושא בעל חשיבות רבה ביותר. בשיעור זה תלמד כיצד לנהל אישורים, לבטל אישור וליישם מדיניות התאוששות עבור EFS (**E**ncrypted **F**ile **S**ystem).

לאחר שיעור זה, תוכל

- לתאר את התהליכים לביטול אישור.
- לתאר כיצד להפעיל מדיניות התאוששות עבור EFS.

זמן לימוד משוער: 30 דקות

אישורים מבוטלים

כאשר אישור מסומן כ״מבוטל״ (Revoked) הוא מועבר לתיקיה Revoked Certificates. האישור המבוטל יופיע ב-CRL בפעם הבאה בה היא תפורסם. אישורים אשר בוטלו באמצעות קוד סיבה (Reason Code) Certificate Held יכולים להיות משוחזרים, להישאר בתיקיה Revoked Certificates עד שתוקפם פג, או עד אשר קוד הסיבה לביטולם משתנה. זהו קוד הסיבה היחיד המאפשר לך לשנות את מצבו של אישור מבוטל. קוד זה יעיל במידה ומצב האישור שנוי במחלוקת, והוא נועד כדי לספק גמישות כלשהי למנהל ה-CA.

אישורים שהונפקו

בחלונית הפרטים (Detail), בחן את הבקשות לאישורים על ידי בדיקת ערכי שם המשתמש, כתובת הדואר האלקטרוני של המשתמש וכל שדה אחר הנחשב למידע חיוני לצורך הפקת אישור.

אישורים בהמתנה

בחלונית הפרטים (Detail), בחן את הבקשות לאישורים על ידי בדיקת ערכי שם המשתמש, כתובת הדואר האלקטרוני של המשתמש וכל שדה אחר הנחשב למידע חיוני לצורך הפקת אישור.

בקשות שכשלו

בקשות לאישורים שכשלו יתרחשו רק כאשר חבר בקבוצה Cert Publishers או בקבוצה Administrators אינו מאשר את הנפקת האישור.

כיצד מונפק אישור

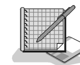
כאשר האישור מוצג בפני יישות כאמצעי לזיהוי מחזיק האישור (נושא האישור), הוא יעיל רק במידה והיישות המקבלת את האישור סומכת על ה-CA שהנפיקה אותו. אישורים מונפקים על פי התהליך הבא:

- **יצירת מפתחות.** המועמד המבקש את האישור מחולל צמד מפתחות, פרטי וציבורי. יוצא מהכלל לכך הוא אישור דיגיטלי אישי, שבמקרה כגון זה מחוללת ה-CA את צמד המפתחות ושולחת אותו למשתמש הקצה.
- **התאמת נתוני מדיניות.** המועמד אורז יחדיו את הנתונים הנדרשים על ידי ה-CA לשם הנפקת האישור (למשל, הוכחת זהות, מספר תיק במס הכנסה, כתובת דואר אלקטרוני וכדומה). המידע המדויק המתבקש הוא לפי שיקול דעתה של ה-CA.
- **שליחת מפתחות ציבוריים ונתונים.** המועמד שולח ל-CA את המפתחות הציבוריים ונתונים נדרשים נוספים (בדרך כלל יתבצע הדבר על ידי הצפנת הנתונים באמצעות המפתח הציבורי של ה-CA).
- **אימות הנתונים.** ה-CA מחילה כללי מדיניות כלשהם הנדרשים לה כדי לוודא שהמועמד אכן יקבל את האישור.
- **יצירת האישור.** ה-CA יוצרת מסמך דיגיטלי עם הנתונים המתאימים (מפתחות ציבוריים, תאריך פקיעת התוקף ומידע נוסף) וחותמת עליו באמצעות המפתח הפרטי של ה-CA.
- **שליחת או הצבת האישור.** ה-CA עשויה לשלוח את האישור למועמד, או שהיא תציב אותו במקום ציבורי. האישור נטען למערכת הקצה של המשתמש.

ביטול אישור

רשויות אישורים מפרסמות רשימות אישורים מבוטלים (**C**ertificate **R**evocation **L**ists ,CRLs) המכילות אישורים שבוטלו על ידי רשות האישורים. ייתכן שהמפתח הפרטי של בעל האישור, או שלשם קבלת האישור ניתנו נתונים שאינם נכונים. CRLs מספקות דרך למשיכת אישור לאחר שהוא הונפק. CRLs זמינות להורדה או לצפייה מקוונת על ידי יישומי לקוח.

כדי לוודא ולאמת אישור, כל שנדרש הוא המפתח הציבורי של ה-CA ובדיקה כנגד רשימת האישורים המבוטלים שפורסמה על ידי ה-CA. אישורים ו-CAs מפחיתים את הבעיתיות שבהפצת מפתח ציבורי לשם וידוא ונתינת אמון במפתח ציבורי אחד (או יותר) לאדם. במקום זאת, יש לתת אמון רק במפתח הציבורי של ה-CA, וזה מאפשר להמשיך ולתת אמון באישורים נוספים.

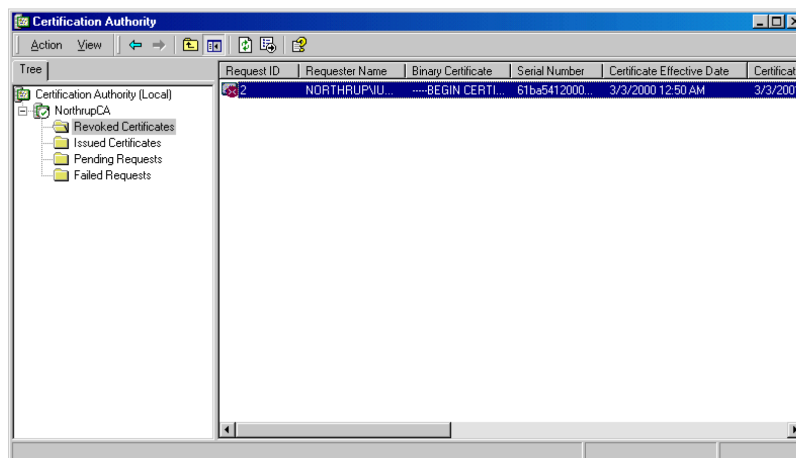


תרגול: ביטול אישור

➢ כדי לבטל את האישור שניתן בשיעור 2

1. פתח את Certificate Authority Manager.
2. לחץ לחיצה ימנית על הבקשה שלך שמתחת ל- Issued Certificates, בתפריט הקיצור הצבע על All Tasks, ובחר Revoke Certificate.
3. כאשר תתבקש לבחור את קוד הסיבה (Reason Code), בחר Cease of Operation, ולחץ Yes.
4. בחלונית השמאלית לחץ על Revoked Certificates.

שים לב שהבקשה שלך בוטלה, כפי שניתן לראות בתרשים 13.5.



תרשים 13.5 אישורים שבוטלו ב- CA

מדיניות שחזור עבור EFS

שחזור נתונים (Data Recovery) זמין עבור EFS כחלק ממכלול מדיניות האבטחה עבור המערכת. לדוגמה, אם אי פעם תאבד את אישור הצפנת הקבצים (File Encryption Certificate) שלך ואת המפתח הפרטי המשויך לה (במקרה של קריסת כונן הדיסק הקשיח או מכל סיבה אחרת), שחזור הנתונים אפשרי על ידי האדם אשר מוגדר כסוכן התאוששות (Recovery Agent). או, בסביבה עסקית, יכול הארגון לשחזר מידע שהוצפן על ידי עובד בארגון, לאחר שזה עוזב את הארגון.

מדיניות שחזור EFS מציינת את החשבונות המוגדרים כסוכני השחזור (Data Recovery Agent) בהם משתמשים בתוך המרחב (Scope). EFS דורשת מדיניות סוכן שחזור נתונים, לפני שניתן יהיה להשתמש בה, ובעצמה משתמשת בחשבון סוכן השחזור המוגדר כברירת מחדל (Administrator) אם לא נבחר אחד אחר. ב-Domain, רק חברים בקבוצה Domain Admins יכולים לייעד חשבון אחר כחשבון סוכן השחזור. בעסק קטן או

משרד ביתי בהם אין domains, ייחשב חשבון המנהל המקומי כסוכן השחזור של ברירת המחדל. רק חשבון המנהל יכול לשנות מדיניות שחזור מקומית עבור המחשב.

חשבון סוכן שחזור משמש לשחזור נתונים עבור כל המחשבים המופיעים במדיניות. אם אבד למשתמש המפתח הפרטי שלו, ניתן לגבות את הקובץ המוגן באמצעות מפתח זה ואת קובץ הגיבוי לשלוח באמצעות דואר מאובטח למנהל סוכן אבטחה. המנהל משחזר את העותק המגובה ופותח אותו, כדי לקרוא את הקובץ, הוא מעתיק את תוכן הקובץ כטקסט פשוט ומחזיר את עותק הטקסט הפשוט למשתמש באמצעות דואר אלקטרוני מאובטח.

כחלופה לכך, יכול מנהל המערכת לגשת באופן פיסי למחשב בו מאוחסן הקובץ המוצפן, לייבא את אישור סוכן השחזור שלו ואת המפתח הפרטי ולבצע את פעולת השחזור ישירות במחשב זה. אבל, פעולה כגון זו עלולה להיות לא בטוחה, וכלל אינה מומלצת, בשל הרגישות היתירה של מפתח השחזור - מנהל המערכת אינו יכול להרשות לעצמו להשאיר את מפתח השחזור במחשב אחר.

 תרגול: שינוי מדיניות השחזור

בתרגול זה תשנה את מדיניות השחזור (Recovery Policy) עבור המחשב המקומי. לפני שתשנה את מדיניות השחזור באופן כלשהו, עליך קודם כל לגבות את מפתחות השחזור לדיסקט. ב-domain, מדיניות ברירת המחדל לשחזור מיושמת עבור ה-domain כולו כאשר מותקן ומוגדר Domain Controller. למנהל ה-domain מונפק אישור חתום באופן עצמי, אשר מטיל על המנהל (Domain Administrator) להיות סוכן השחזור (Recovery Agent). כדי לשנות את מדיניות ברירת המחדל לשחזור עבור doamin, היכנס ל-DC הראשון באמצעות חשבון מנהל (Administrator).

הערה כדי להשלים תרגול זה צריכות להיות לך ההרשאות המתאימות כדי לבקש את האישור וה-CA צריכה להיות מוגדרת להנפיק סוג זה של אישור.

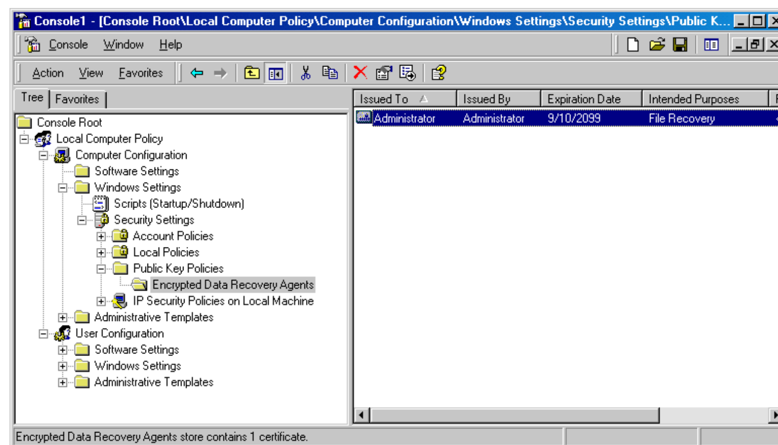
➢ כדי לשנות את מדיניות השחזור עבור המחשב המקומי

1. לחץ Start, לחץ Run. בתיבת הטקסט Open הקלד את הפקודה mmc /a, ולחץ OK.
2. פתח את תפריט Console, בחר Add/Remove Snap-In, ולחץ Add.
3. מהרשימה Snap-In בחר Group Policy, ולחץ Add.
4. תחת Group Policy Object ודא שמוצגת האפשרות Local Computer, ולחץ Finish. לחץ Close, ואחר כך לחץ OK.
5. תחת Navigate Local Computer Policy, Computer Configuration, Windows Settings, Security Settings, Public Key Policies, לחץ לחיצה ימנית על Encrypted Data Recovery Agents ומתפריט הקיצור המופיע בחר באחת מהאפשרויות הבאות:

   הפקודה Add מטילה על משתמש לשמש כסוכן שחזור נוסף, תוך שימוש באשף Add Recovery Agent Wizard. הפקודה Delete Policy מוחקת את מדיניות EFS הנוכחית ואת כל סוכני השחזור. השפעת מחיקת מדיניות EFS וכל סוכני השחזור על

המשתמשים היא, שהם לא יוכלו להצפין קבצים במחשב זה. המחשבי מנפיק אישור ברירת מחדל חתום באופן עצמי המייעד את המנהל המקומי כסוכן ברירת המחדל לשחזור. אם תמחק את אישור זה מבלי שתהיה מדיניות אחרת במקומה, נותר המחשב עם מדיניות שחזור ריקה. מדיניות שחזור ריקה משמעותה שאף אחד אינו סוכן שחזור. במקרה כגון זה EFS מנוטרלת ואינה פעילה, וכך אינה מאפשרת למשתמשים להצפין קבצים במחשב זה.

6. כדי לבצע שינויים באישור File Recovery, התחל בבחירת Encrypted Data Recovery Agents בחלונית השמאלית, כפי שניתן לראות בתרשים 13.6. לחץ לחיצה ימנית על האישור בחלונית הימנית ומתפריט הקיצור בחר Properties. לדוגמה, תוכל לתת לאישור שם ידידותי ולהוסיף טקסט תיאור עבורו.



תרשים 13.6 מדיניות קבוצתית עבור שחזור EFS

סיכום שיעור

תוכל לנהל אישורים ב-MMC תוך שימוש בישום Snap-In בשם Certification Authority. אישורים המבוטלים כאשר קוד הסיבה המוגדר להם הוא Certificate Held יכולים להיות משוחזרים. ניתן אף להשאירם בתיקיה Certificate Held עד שפג תוקפם, או שקוד הסיבה לביטולם משתנה. שחזור נתונים עבור EFS זמין כחלק ממכלול מדיניות האבטחה של המערכת.

שאלות סיכום

השאלות הבאות נועדו לחזק את הנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות על שאלה, עיין בשיעור המתאים ונסה את השאלה שנית. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואחר כך בעברית.

Answering the following questions will reinforce key information presented in this chapter. If you are unable to answer a question, review the appropriate lesson and then try the question again. Answers to the questions can be found in Appendix A, "Questions and Answers."

1. What are certificates, and what is their purpose?
2. What is a certificate authority (CA), and what does it do?
3. What are the four types of Microsoft certificate authorities?
4. Name one reason for a certificate revocation.
5. What are the five PKI standard certificate stores?

1. מהם אישורים ומה מטרתם?
2. מהי רשות אישורים (CA) ומה היא עושה?
3. מהם ארבעת הסוגים של רשויות האישורים של Microsoft.
4. מנה סיבה אחת לביטול אישור.
5. מהם חמשת המחסנים התקניים לאחסון PKI?

פרק 14

יישום אבטחת רשת
ברמת הארגון

אודות פרק זה

בפרק זה תלמד כיצד ליישם אבטחה ברשת שלך וכיצד לתכנן כראוי את נושא האבטחה. בנוסף תלמד כיצד להקים ולאבטח קישורים מרחוק לרשת שלך. מעבר לכך, יידונו בפרק זה נושאי ניטור ואיתור וטיפול בתקלות במשאבי רשת ובגישה מרחוק.

לפני שתתחיל

להשלמת פרק זה צריך שיהיה ברשותך:

- ❖ מחשב בו מותקנת מערכת ההפעלה Windows 2000 Server.
- ❖ להשלים את הפרקים 2 עד 10.

שיעור 1: יישום אבטחת רשת

בעת תכנון הרשת שלך עליך ליישם טכנולוגיות אבטחה המתאימות לארגון שלך. הגישה לנושאים אלה בשלבים המוקדמים של תכנון ההגירה לסביבת Windows 2000, תבטיח שלא ייווצרו חורי אבטחה (Security Breaches) וכי תהיה מסוגל לספק רשת מאובטחת במידת הצורך. בשיעור זה תלמד כיצד ליישם אבטחה ברשת שלך.

לאחר שיעור זה, תוכל

- לתאר חלקים בתוכנית האבטחה של הרשת.
- לזהות סכנות באבטחת הרשת.
- לתאר את תכונות האבטחה של Windows 2000.
- לתאר כיצד לאבטח את החיבור בין הרשת שלך והאינטרנט.

זמן לימוד משוער: 35 דקות

תכנון אבטחת הרשת

אפילו אם אתה בטוח שיישמת סביבת רשת מאובטחת, חשוב שתסקור את אסטרטגיית האבטחה שלך בהתאם לאפשרויות של Windows 2000. חלק מטכנולוגיות האבטחה החדשות ב- Windows 2000 עשויות לגרום לך לבצע תכנון מחדש של תוכנית האבטחה. בעודך מפתח את תוכנית האבטחה שלך עליך:

- ❖ לאמוד את סיכוני האבטחה של הרשת.
- ❖ לקבוע את דרישות גודל השרת שלך ומיקומו.
- ❖ להכין את הצוות שלך.
- ❖ ליצור ולפרסם נהלים ומדיניות אבטחה.
- ❖ להשתמש במתודולוגיה רשמית ליצירת תוכנית יישום לטכנולוגיות האבטחה בהן תשתמש.
- ❖ לזהות את קבוצות המשתמשים שלך, את צרכיהן המיוחדים ואת סיכוני האבטחה הכרוכים באותם צרכים.

אומדן סיכוני האבטחה ברשת

למרות שהאפשרות לשתף ולהשיג מידע עשויה להיות יעילה ביותר, היא גם מציגה מספר סיכוני אבטחה. אלה מתוארים בטבלה 14.1.

טבלה 14.1 סיכונים באבטחת רשת

סיכון אבטחה	תיאור
Identity Interception	הפולש מגלה את שם המשתמש וסיסמתו של משתמש חוקי. דבר זה עשוי להתבצע במיגוון שיטות, טכניות ואנושיות.
Masquerade	משתמש שאינו מורשה מתחזה למשתמש חוקי. לדוגמה, משתמש מקבל כתובת IP של מערכת הנחשבת לבטוחה ומשתמש בה כדי לקבל את הרשאות הגישה הניתנות להתקן או מערכת מתחזה.
Replay Attack	הפולש קולט חילופי נתונים בין משתמש חוקי לשרת, ומפעיל אותם פעם נוספת בשלב מאוחר יותר, כדי להתחזות לאותו משתמש.
Data Interception	אם נתונים מועברים ברשת כטקסט פשוט (Plaintext), יכול משתמש שאינו מורשה לכך לנטר וללכוד את הנתונים הללו.
Manipulation	הפולש גורם לשינויים או להרס נתונים המועברים ברשת. נתוני עסקאות שאינם מוצפנים רגישים במיוחד לסוג מתקפה כזה.
Repudiation	עסק מבוסס-רשת ועסקאות כלכליות עשויים למצוא פשרה, במידה ומקבל נתוני העסקה אינו בטוח בשולח הנתונים.
Macro Viruses	וירוסים ייחודיים ליישום עשויים לנצל את שפת המאקרו של מסמכים וגיליונות מורכבים.
Denial of Service	הפולש עלול להציף את השרת בבקשות אשר מכלות את משאבי המערכת ועקב כך גורם לקריסת המערכת, או מונע ממנו מלבצע את עבודתו כראוי.
Malicious Mobile Code	מונח זה מתייחס לקוד הרסני המופעל באמצעות פקדי ActiveX או יישומוני Java הנטענים מהאינטרנט לשרת האינטרנט.
Misuse of Privileges	מנהל מערכת, באופן מודע או שלא מודע, משתמש בזכויות המערכת המלאות שניתנו לו כדי לחדור למידע אישי/פרטי.
Trojan Horse	זהו מונח כללי לתוכנית הרסנית המתחזה לתוכנית שירות בלתי מזיקה.
Social Engineering Attack	לעיתים, כל שנדרש לשם פריצה לרשת הוא להתקשר לעובד חדש בחברה, להגיד לו שאתה מצוות מנהלי המערכת ולבקש ממנו לוודא את הסיסמה עבור רישומי המחלקה.

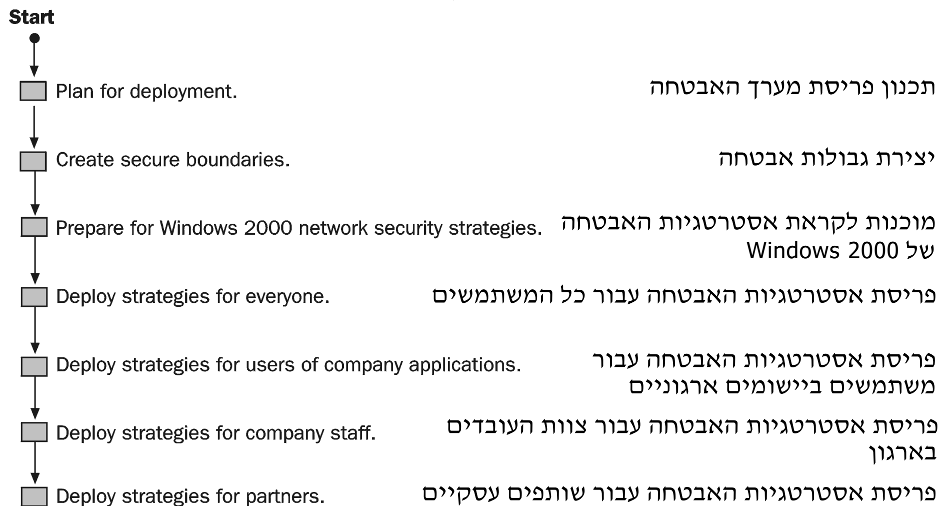
מתחרים עסקיים עשויים לנסות להשיג דרכי גישה למידע רגיש אודות מוצרי החברה, או שמשתמשים שאינם מורשים לכך עשויים לנסות לשנות דפי אינטרנט, או להעמיס על המחשבים באופן כזה שיהפכו ללא שמישים. מעבר לכך, עובדי החברה עשויים לגשת למידע חסוי. חשוב למנוע סוגים כאלה של סיכוני אבטחה, כדי להבטיח שהתפקודיות העסקית של הארגון לא תיפגע.

אימות רשת

אימות (Authentication) הוא התהליך של זיהוי משתמשים המנסים להתחבר לרשת. משתמשים אשר מאומתים ברשת יכולים לנצל משאבי רשת בהתאם להרשאות הגישה שלהם. כדי לספק אימות למשתמשי הרשת עליך ליצור חשבונות משתמשים. דבר זה הכרחי לשם ניהול אבטחת המידע בארגון. ללא אימות, משאבים כגון קבצים עשויים להיות נגישים גם למשתמשים שאינם מורשים בכך.

תוכנית אבטחת הרשת

כדי לוודא שרק למשתמשים המתאימים תתאפשר הגישה למשאבים ולנתונים, עליך לתכנן היטב את אסטרטגיית האבטחה של הרשת שלך. דבר זה מאפשר גם לקיים מעקב אחר אופן השימוש במשאבי הרשת. תרשים 14.1 מתאר את הצעדים העיקריים לקבלת החלטות לגבי אסטרטגיית האבטחה ברשת שלך.



תרשים 14.1 צעדים עיקריים לקבלת החלטות לגבי אסטרטגיית אבטחת הרשת

הכנת הצוות

טכנולוגיות אבטחה צריכות להיפרס ולהיות מנוהלות על ידי צוות מיומן ונאמן. עליהם לשלב את תשתית הרשת והאבטחה באופן כזה שיאפשר לך למנוע או להקטין את חולשות המערכת. בעוד סביבת העבודה והדרישות משתנות, עליהן לשמר באופן רציף את שלמות תשתית אבטחת הרשת.

גורם מכריע בהבטחת הצלחת צוות אבטחת הרשת שלך הוא להבטיח שהצוות כולו מיומן בתפקידו, ומודע לשינויים בטכנולוגיות האבטחה. על כל אנשי הצוות ללמוד להכיר את Windows 2000 מקרוב, ובמיוחד את נושא טכנולוגיות אבטחת הרשת בסביבת עבודה זו. צריכה גם להיות להם ההזדמנות לאכוף את הידע שהם רוכשים בלימודיהם בעבודה עם רשתות ניסיוניות, ויישום הידע שלהם ברשתות קיימות. תכונות האבטחה של Windows 2000 מתוארות בטבלה 14.2.

טבלה 14.2 תכונות האבטחה של Windows 2000

תכונה	תיאור
Security Templates	מאפשרות למנהלי מערכת לקבוע הגדרות אבטחה גלובליות או מקומיות, כולל ערכי רישום מערכת (Registry) הרגישים מבחינת אבטחה; בקרת גישה לקבצים ולערכי רישום; יישום אבטחה לגבי שירותי מערכת.
Kerberos Authentication	פרוטוקול האבטחה העיקרי בתוך ובין Windows 2000 domains. מספק אימות הדדי של לקוחות ושרתים, ותומך בהאצלת סמכויות ואימות באמצעות מנגנוני Proxy.
Public Key Infrastructure (PKI)	ניתן להשתמש ב-PKI המשולב להגברת האבטחה בין מיגוון שירותי אינטרנט של Windows 2000 ושירותים אירגוניים, כולל תקשורת מבוססת אקסטראנט.
Smart Card Infrastructure	Windows 2000 כוללת מודל תקני לתקשורת עם קוראי כרטיסים חכמים וכרטיסים עם מחשבים וממשקי תכנות יישומים שאינם תלויי-התקן, כדי לאפשר הפעלת יישומים המודעים לכרטיסים חכמים.
IP Security Protocol (IPSec) Management	IPSec תומך באימות ברמת הרשת, שלמות נתונים והצפנה של תקשורת אינטרנט / אינטראנט / אקסטראנט.
NT File System (NTFS) Encryption	ניתן ליישם אבטחת NTFS מבוססת מפתח ציבורי על בסיס קובץ או תיקיה.

למרות שטכנולוגיות אבטחה עשויות להיות יעילות מאוד, אבטחה בעצמה משלבת טכנולוגיות אלו עם תפקוד עסקי או חברתי נאות. לא חשוב כמה מתקדמת ועד כמה טוב היא יושמה, הטכנולוגיה טובה רק כמו השיטות בהן השתמשו לפרוס ולנהל אותה.

תכנון אבטחת רשת מבוזרת

אבטחת רשת מבוזרת (Distributed Network Security) מערבת בחובה את התיאום בין פעילויות אבטחה רבות במחשב מרושת, כדי ליישם מדיניות אבטחה כוללת. אבטחה מבוזרת מתירה למשתמשים להיכנס למערכת (Logon) למערכת המחשבים המתאימה ומאפשרת להם לאתר ולהשתמש במידע לו הם זקוקים. רוב המידע העובר ברשת תקשורת מחשבים ניתן לצפייה על ידי כולם, אך רק חלק מצומצם של משתמשים מורשים לעדכן מידע זה. אם המידע הוא רגיש או חסוי, רק משתמשים מורשים או קבוצות משתמשים מסוימות מאוד מורשים לקרוא קבצים אלה. יש לשקול את ההגנה והפרטיות של המידע המועבר ברשתות טלפוניה ציבוריות (האינטרנט), ואפילו קטעים של הרשת הפנים-ארגונית. נושא זה נדון בהרחבה בשיעור 2 של פרק זה.

תוכנית אבטחה טיפוסית כוללת חלקים כגון אלה המוצגים בטבלה 14.3. אבל, עליך לזכור שפריסת האבטחה ברשת שלך עשויה לכלול חלקים נוספים. חלקי התכנון המופיעים בטבלה מומלצים כמינימום ההכרחי בלבד.

טבלה 14.3 תכונות האבטחה של Windows 2000

החלק בתכנון	תיאור
סיכוני אבטחה	מניית סוגי סיכוני האבטחה העשויים להשפיע על הארגון.
אסטרטגיות אבטחה	מתאר באופן כללי את אסטרטגיות האבטחה הנחוצות כדי לעמוד בפני הסיכונים.
מדיניות PKI	כולל את התוכנית לפריסת רשויות מאשרות (CA) עבור תכונות האבטחה הפנימיות והחיצוניות.
תיאורי קבוצות אבטחה	כולל תיאורים של קבוצות אבטחה ואופי היחסים ביניהן. חלק זה ממפה מדיניות קבוצתיות לקבוצות אבטחה.
מדיניות קבוצתית	כולל כיצד תגדיר את הגדרות האבטחה של Group Policy, כגון מדיניות הסיסמאות ברשת.
אסטרטגיות התחברות לרשת ואימות	כולל אסטרטגיות אימות עבור התחברות לרשת ועבור השימוש בגישה מרחוק ובכרטיסים חכמים לצורך התחברות למערכת. נושא זה נדון בהרחבה בשיעור 2.
אסטרטגיות אבטחת מידע	כולל את האופן בו תיישם פתרונות אבטחת מידע, כגון דואר אלקטרוני מאובטח ותקשורת אינטרנטית מאובטחת.
מדיניות ניהול	כולל המדיניות להאצלת סמכויות לביצוע משימות ניהוליות וניטור יומני ביקורת, כדי לבחון ולאתר פעילות חשודה.

מעבר לכך, ייתכן שלארגון שלך תידרש יותר מאשר תוכנית אבטחה יחידה. מספר התוכניות שתהיינה לך תלוי במרחב הפריסה שלך. ארגון בינלאומי עשוי לתכנן תוכנית נפרדת לכל אחת מהמחלקות או המיקומים העיקריים שלו, בעוד שארגון אזורי עשוי להזדקק לתוכנית אחת בלבד. ארגונים להם מדיניות ברורות לכל קבוצת משתמשים, עשויים להידרש לתוכנית אבטחה לכל אחת מהקבוצות.

בדיקת תוכנית האבטחה שלך

תמיד עליך לבחון, לבדוק ולשנות את תוכנית אבטחת הרשת שלך באמצעות מעבדות בדיקה המדמות את סביבת המחשוב בארגון. בנוסף, עליך לנהל תוכנית פילוט (Pilot) כדי לבדוק ולמטב את תוכנית האבטחה הראשונית.

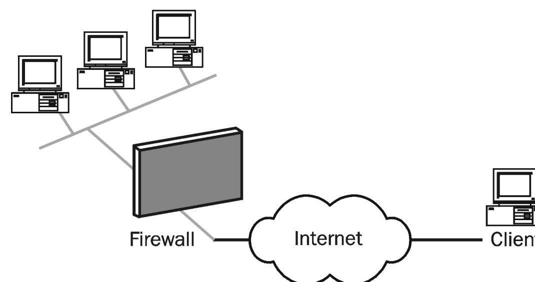
חיבוריות לאינטרנט

כיום, מרבים הארגונים מעוניינים שתשתית המחשוב שלהם תהיה מחוברת לרשת האינטרנט בחיבור קבוע, מפני שהיא מספקת שירותים חשובים הן לעובדים בארגון והן ללקוחותיו. חיבור לאינטרנט מאפשר לעובדים בארגון להשתמש בדואר אלקטרוני, כדי לתקשר עם אנשים מסביב לעולם ולהשיג מידע וקבצים ממספר גדול של מקורות. חיבור

זה גם מאפשר ללקוחותיך לקבל מידע ושירותים מהארגון בכל עת. בנוסף, העובדים בארגון יכולים להשתמש במשאבי הארגון מביתם, ממלון או מכל מקום אחר בו הם עשויים לשהות. שותפים עסקיים עשויים להשתמש באמצעים המיוחדים שיועמדו לרשותם, כדי לעבוד באופן יעיל יותר עם הארגון שלך. אבל, באותם שירותים העומדים לרשות משתמשים דרך האינטרנט ניתן גם לעשות שימוש שאינו הולם. דבר זה יוצר את הצורך ביישום אסטרטגיות אבטחה ברשת.

יישום חומת אש

כדי להגן על רשת הארגון מפני גישה אל ומהאינטרנט, עליך להקים חומת אש (Firewall) ביניהם, כפי שמתואר בתרשים 14.2. חומת האש מספקת חיבוריות לאינטרנט עבור עובדי הארגון, בעודה ממזערת את הסכנות שחיבוריות כגון זו יוצרת. באותו זמן היא גם מונעת גישה מהאינטרנט למחשבים ברשת שלך, חוץ מאשר אותם מחשבים המורשים לגישה כגון זו.



תרשים 14.2 חומת אש - Firewall

חומת אש מיישמת סינון מנות (Packet Filtering) המאפשר או מונע את הזרימה של תעבורת רשת מסוימת מאוד. סינון מנות IP מספק לך דרך להגדיר בדיוק איזו תעבורת IP מורשית לעבור דרך חומת האש. סינון מנות IP הוא נושא חשוב כאשר אתה מחבר רשתות אינטראנט פרטיות לרשת האינטרנט הציבורית. חומות אש רבות מסוגלות גם לזהות ולהגן מפני התקפות מורכבות.

בדרך כלל פועלות חומות אש גם כשרתי Proxy או כנתבים, מפני שהן מעבירות תעבורה בין הרשת הציבורית לרשת הפרטית. תוכנת חומת האש או שרת ה-Proxy בוחנים את כל מנות הרשת בכל ממשק, כדי לקבוע את כתובת היעד שלהן. אם המנה עומדת בקריטריונים מסוימים, תאפשר חומת האש למנה להיות מועבר ליעדה באמצעות ממשק הרשת השני שלה. חומת האש עשויה פשוט לנתב מנות, או שהיא עשויה לפעול כשרת Proxy ותתרגם את כתובות ה-IP ברשת הפרטית.

שרת Proxy של Microsoft

Microsoft Proxy Server משמש הן כשרת Proxy והן מעין חומת אש (Firewall). שרת Proxy מופעל במחשב Windows 2000, ושניהם חייבים להיות מוגדרים כהלכה כדי לספק אבטחה מלאה לרשת. אם ברשותך גירסה קודמת לגירסה 2.0 עם חבילת שירות 1 (Service Pack 1)

יהיה עליך לשדרג את גירסת התוכנה, כדי להתאימה לעבודה עם Windows 2000. עשה זאת כחלק מההגירה לסביבת Windows 2000.

במקרים רבים, כמות תעבורת הנתונים שבין הרשת הארגונית לבין רשת האינטרנט גדולה מכדי שרק שרת proxy אחד יוכל לטפל בה. במקרים כגון אלה עליך להשתמש במספר שרתי Proxy; התעבורה מתואמת ביניהם באופן אוטומטי. למשתמשים משני הקצוות (האינטראנט והאינטרנט) נראה כאילו קיים רק שרת Proxy אחד.

הערה התהליכים לשימוש ב- Microsoft Proxy Server נכללים במוצר. למידע נוסף אודות Microsoft Proxy Server ולפרטים נוספים אודות טכנולוגיות אבטחה, פנה לקישור עבור Microsoft Security Advisor שבדף האינטרנט Web Resources שכתובתו:

http://www.microsoft.com/windows2000/library/resources/reskit/WebResources/default.asp

---

כאשר סיימת להתקין ולהגדיר שרת Proxy, כולל את אמצעי הניטור וצוות מיומן כהלכה, תוכל לחבר את הרשת שלך לרשת חיצונית. עליך להיות בטוח שרק השירותים שהגדרת יהיו זמינים, וכי הנזק של שימוש לרעה כמעט ואינו קיים. סביבה זו אמנם זקוקה לניטור ותחזוקה קפדניים ביותר, אך היא מכינה אותך גם לאספקת שירותי רשת מאובטחים נוספים.

סיכום שיעור

עליך לתכנן את אסטרטגיות האבטחה שלך כדי לוודא שרק לאנשים המתאימים יש גישה למשאבים ולנתונים ברשת. בנוסף על כך, עליך ליישם טכנולוגיות אבטחה המתאימות לארגון שלך. תמיד בדוק והתאם את תוכניות האבטחה לרשת, תוך שימוש במעבדות בדיקה המדמות את סביבת המחשוב בארגון. תוכל ליישם חומת אש (Firewall) כדי לאבטח את רשת הארגון שלך מפני גישה אל ומהאינטרנט. כאשר הוא פועל במחשב Windows 2000 Server, מספק שרת ה-Proxy של Microsoft הן יכולות של חומת אש והן יכולות של שרת Proxy.

שיעור 2:
הגדרת אבטחת ניתוב וגישה מרחוק

גישה מרחוק מאפשרת ללקוחות להתחבר לרשת שלך ממיקום מרוחק באמצעות התקני חומרה מגוונים, הכוללים בין היתר כרטיסי רשת ומודמים. לאחר שלקוחות הקימו חיבור בגישה מרחוק הם יכולים להשתמש במשאבי הרשת, כגון קבצים, באותו אופן בו עושים זאת מחשבי לקוח המחוברים ישירות לרשת המקומית (LAN). בשיעור זה תלמד כיצד להגדיר אבטחה עבור גישה מרחוק לרשת שלך.

לאחר שיעור זה, תוכל

- ליצור מדיניות גישה מרחוק.
- להגדיר אבטחת גישה מרחוק.
- להגדיר פרוטוקולי הצפנה.
- להגדיר פרוטוקולי אימות.
- להגדיר, לאתר ולטפל בתקלות באבטחת פרוטוקולי הרשת.

זמן לימוד משוער: 60 דקות

סקירת הגישה מרחוק

כפי שלמדת בפרק 11, Routing and Remote Access הוא השירות המאפשר למשתמשים מרוחקים להתחבר לרשת המקומית שלך באמצעות הטלפון. גישה מרחוק מספקת לפולשים לא רצויים הזדמנות גישה לרשת שלך; בשל כך, מספקת Windows 2000 מיגוון תכונות אבטחה כדי לאפשר גישה מורשית מרחוק בעודה מונעת את הפולשים המזדמנים. כאשר לקוח מחייג לשרת הגישה מרחוק של הרשת שלך, הוא יקבל גישה לרשת אם הוא עומד בתנאים הבאים:

- הבקשה תואמת לאחת ממדיניות הגישה מרחוק המוגדרות בשרת.
- חשבון המשתמש מאפשר גישה מרחוק.
- אימות שרת/לקוח מצליח.

לאחר שהלקוח הזדהה ואושר, ניתן להגביל את הגישה לשרתים מסוימים ברשת, לרשתות משנה מסוימות ולסוגי פרוטוקולים, בהתאם לפרופיל הגישה מרחוק של המשתמש. אחרת, כל השירותים אשר בדרך כלל זמינים עבור לקוח המחובר לרשת המקומית (LAN), כולל שיתוף קבצים והדפסה, גישה לשרת האינטרנט ושירותי ההודעות, יהיו זמינים גם למשתמשים המחוברים בגישה מרחוק.

הגדרת פרוטוקולים לאבטחה

בעוד שמשתמש מנסה להיכנס לשרת הגישה מרחוק, יכול מישהו לנסות לשים את ידו על שם המשתמש והסיסמה באמצעים של האזנה לחוטים (Wiretrap). כדי למנוע זאת, יכול שירות Routing and Remote Access להשתמש בשיטת אימות מאובטחת, כגון:

- **CHAP (Challenge Handshake Authentication Protocol).** CHAP נועד לטפל בבעיית העברת ססמאות כטקסט רגיל (Plaintext). מבחינה היסטורית, CHAP הוא פרוטוקול האימות השכיח ביותר לאימותי Dial-up. מכיון שאלגוריתם החישוב של תגובות CHAP ידוע לרבים, חשוב מאוד שהססמאות ייבחרו בקפידה, ושהן תהיינה ארוכות מספיק. ססמאות CHAP שהן מילים מקובלות או שמות, הן הרגישות ביותר בפני התקפות מילון (Dictionary Attacks) אם הן ניתנות לגילוי על ידי השוואת התגובות לאתגרי CHAP (CHAP Challenge) למילים במילון. ססמאות שאינן ארוכות דיין יכולות להתגלות באמצעות Brute Force על ידי השוואת תגובת CHAP לניסיונות רציפים, עד אשר נמצאת התאמה לתגובת המשתמש.
- **MS-CHAP (Microsoft Challenge Handshake Authentication Protocol).** MS-CHAP הוא וריאציה של CHAP שאינה דורשת גרסת טקסט רגיל של הסיסמה בשרת האימות. ססמאות MS-CHAP מאוחסנות באופן מאובטח יותר בשרת, אך קיימים לגביהן אותם הסיכונים להתקפות מילון ו- Brute Force, כמו CHAP. ב- MS-CHAP תגובת האתגר (Challenge Response) מחושבת באמצעות גירסה Hashed של MD4 (Message Digest 4) של אתגרי הסיסמה ושרת הגישה לרשת (NAS, **N**etwork **A**ccess **S**erver). דבר זה מאפשר אימות דרך האינטרנט ל-DC של Windows 2000 (או DC של Windows NT 4.0 בו לא הותקן העדכון).
- **PAP (Password Authentication Protocol).** PAP מעביר סיסמה כמחרוזת (String) ממחשב המשתמש להתקן NAS. כאשר ה-NAS מעביר את הסיסמה, היא מוצפנת תוך שימוש בסוד המשותף של RADIUS (Remote Access Dial-Up Service Shared Secret) כמפתח ההצפנה. PAP הוא הפרוטוקול הגמיש ביותר, מפני שהעברת סיסמה בטקסט רגיל לשרת האימות מאפשרת לשרת זה להשוות את הסיסמה עם כמעט כל מבנה אחסון מוכר. לדוגמה, ססמאות UNIX מאוחסנות כמחרוזת מוצפנת באופן חד-כיווני, אשר אינה ניתנת לפיענוח. ססמאות PAP יכולות להיות מושוות למחרוזת זו על ידי יצירה מחדש של שיטת ההצפנה. מכיון ו-PAP עושה שימוש בגרסת הטקסט הרגיל של הסיסמה יש לו מספר פגיעויות אבטחה. למרות שפרוטוקול RADIUS מצפין את הסיסמה, היא עדיין מועברת כטקסט רגיל דרך קווי החיוג.
- **SPAP (Shiva Password Authentication Protocol).** SPAP הוא מנגנון הצפנה הפיך המיושם בשרתי גישה מרחוק של Shiva. לקוח גישה מרחוק של Windows 2000 יכול להשתמש ב-SPAP כדי לאמת את עצמו בפני שרת גישה מרחוק של Windows 2000. SPAP הוא פרוטוקול מאובטח יותר מאשר PAP, אך עדיין מאובטח פחות מאשר CHAP או MS-CHAP. SPAP אינו מציע הגנה כלשהי מפני התחזות כשרת גישה מרחוק (Remote Server Impersonation).

בדומה ל-PAP, גם SPAP הוא חלופה פשוטה של הודעות. ראשית, לקוח הגישה מרחוק שולח הודעת בקשה לאימות SPAP (SPAP Authenticate-Request) לשרת הגישה מרחוק המכיל את שם המשתמש של לקוח הגישה מרחוק, ואת סיסמתו המוצפנת. אחר כך, שרת הגישה מרחוק מפענח את הסיסמה, בוחן את שם המשתמש ואת סיסמתו ושולח חזרה ללקוח הודעת SPAP Authenticate-Ack (אישור אימות) כאשר נתוני המשתמש מאומתים ונמצאים כנכונים, או הודעת SPAP Authenticate-Nak (אי-אישור האימות) הכוללת את הסיבה לכך שנתוני המשתמש אינם תואמים.

- **EAP (Extensible Authentication Protocol).** EAP הוא הרחבה של פרוטוקול PPP (Point-to-Point Protocol) המוכר, אשר מאפשר ליישם מנגנוני אימות מתוחכמים (Arbitrary Authentication Mechanisms) לשם אימותם של חיבורי PPP. במקרה של פרוטוקולי אימות PPP כגון MS-CHAP ו- SPAP, נבחר מנגנון אימות מסוים בשלב הקמת החיבור (Connection Establishment). אז, במהלך שלב אימות החיבור (Connection Authentication), משמש פרוטוקול האימות עליו הוסכם כדי לאמת את החיבור עצמו. פרוטוקול האימות עצמו הוא קבוצות קבועות של הודעות הנשלחות בסדר מסוים. מבחינת הארכיטקטורה, EAP נועד לאפשר מודולי Plug-in של אימות משני קצות החיבור, הן בשרת והן בלקוח. על ידי התקנת קובץ ספריה מסוג EAP משני צידי החיבור (בשרת הגישה מרחוק ובלקוח הגישה מרחוק), ניתן לתמוך בסוג חדש של EAP. אפשרות זו מציבה בפני היצרנים את ההזדמנות לספק סכמת אימות חדשה בכל עת. EAP מספק את הגמישות הרבה ביותר בייחודיות האימות לסוגיו.

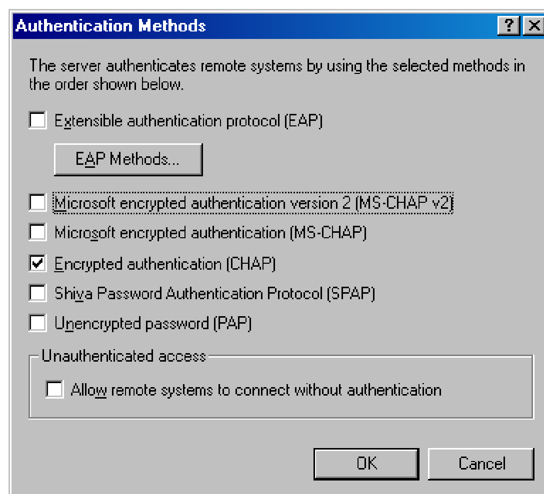
תרגול: שימוש בפרוקולי אבטחה לחיבור VPN

כדי לאפשר לשרת VPN שלך להשתמש בשיטת האימות של CHAP

1. לחץ על Start, הצבע על Programs, הצבע על Administrative Tools, ולחץ על Routing and Remote Access.
2. לחץ לחיצה ימנית על שם השרת בו אתה מעוניין לאפשר פרוטוקולי אימות, ומתפריט הקיצור בחר Properties.

   מופיעה תיבת דו-שיח Properties של השרת הנבחר.
3. בחר בכרטיסיה Security, ולחץ על Authentication Methods.

   מופיעה תיבת דו-שיח Authentication Methods.
4. בתיבת דו-שיח Authentication Methods סמן את תיבת הסימון Encrypted Authentication , כפי שמוצג בתרשים 14.3, ולחץ OK.
5. לחץ OK כדי לסגור את תיבת דו-שיח Properties של השרת הנבחר.



תרשים 14.3 שימוש בשיטת האימות CHAP

יצירת מדיניות גישה מרחוק

Routing and Remote Access ו-IAS (**I**nternet **A**uthentication **S**ervice) של Windows 2000 משתמשים שניהם במדיניות גישה מרחוק, כדי לקבוע האם יש לקבל או לדחות את ניסיון ההתחברות. בשני המקרים, מדיניות הגישה מרחוק מאוחסנות באופן מקומי. המדיניות מוקדשת כעת על בסיס שיחה (Per-Call).

במדיניות גישה מרחוק תוכל לאפשר או למנוע אישור על פי השעה ביום או היום בשבוע, על פי הקבוצה אליה שייך המשתמש המבצע גישה מרחוק, על פי סוג החיבור המבוקש (חיבור בחיוג או חיבור VPN) וכיוצא באלה.

ניהול מקומי מול ניהול מרכזי של מדיניות

מאחר ומדיניות הגישה מרחוק מאוחסנות באופן מקומי, בין אם בשרת הגישה מרחוק ובין אם בשרת IAS, כדי לנהל במרוכז קבוצה יחידה של מדיניות גישה מרחוק עבור מספר שרתי גישה מרחוק או שרתי VPN, עליך לבצע את הפעולות הבאות:

1. התקן את IAS במחשב Windows 2000 כשירות RADIUS.
2. הגדר את IAS עם לקוחות RADIUS התואמים במדויק לשרתי הגישה מרחוק ושרתי VPN של Windows 2000.
3. בשרת IAS, צור קבוצה מרכזית של מדיניות בהן משתמשים כל שרתי הגישה מרחוק של Windows 2000.
4. הגדר כל אחד משרתי הגישה מרחוק של Windows 2000 כלקוחות RADIUS של שרת IAS.

לאחר שהגדרת את שרת הגישה מרחוק של Windows 2000 כלקוח RADIUS של שרת IAS, לא נעשה יותר שימוש במדיניות הגישה מרחוק המקומיות, המאוחסנות בשרת הגישה מרחוק. השימוש בניהול מרכזי של מדיניות גישה מרחוק מתבצע גם כאשר חלק משרתי הגישה מרחוק הם שרתים מבוססי Windows NT 4.0, בהם מותקן השירות RRAS (**R**outing and **R**emote **A**ccess **S**ervice). ניתן להגדיר שרת מבוסס Windows NT 4.0 בו מותקן שירות RRAS כלקוח לשרת IAS. לעומת זאת, לא ניתן להגדיר שרת גישה מרחוק מבוסס Windows NT 4.0 בו לא מותקן שירות RRAS כך שינצל את היתרונות של מדיניות גישה מרחוק מרוכזות.

שימוש בפרוטוקולי הצפנה

אתה יכול להשתמש בהצפנת נתונים כדי להגן על נתונים הנשלחים בין לקוח גישה מרחוק לבין שרת הגישה מרחוק. הצפנת נתונים היא דבר חשוב עבור מוסדות כלכליים, כוחות ביטחון וסוכנויות ממשלתיות, וגם עבור ארגונים הדורשים העברת נתונים מאובטחת. בהתקנות במקומות בהם סודיות הנתונים היא חיונית, יכול מנהל המערכת להגדיר ששרת הגישה מרחוק ידרוש תקשורת מוצפנת. משתמשים המתחברים לשרת זה חייבים להצפין את הנתונים שלהם, או שניסיון החיבור ייכשל.

עבור חיבורי VPN (**V**irtual **P**rivate **N**etworking), אתה מגן על הנתונים על ידי הצפנתם בין שני קצות ה-VPN. לחיבורי VPN עליך תמיד להשתמש בהצפנת נתונים, כאשר נתונים פרטיים מועברים באמצעות רשת ציבורית, כגון האינטרנט, בה קיימת הסכנה התמידית שייראו על ידי מי שאינו מורשה בכך.

עבור חיבורי רישות בחיוג (Dial-up Networking), תוכל להגן על הנתונים שלך באמצעות הצפנה בקישור התקשורת שבין שרת הגישה מרחוק ולקוח הגישה מרחוק. עליך להשתמש בהצפנת נתונים כאשר קיים חשש שמשתמש שאינו מורשה בכך מאזין לתשדורות הרשת בין השרת והלקוח. קיימות שתי צורות הצפנה הזמינות עבור חיוג-על-פי-דרישה (Demand-Dial) : MPPE (**M**icrosoft **P**oint-to-**P**oint **E**ncryption) ו-IPSec (**IP Sec**urity).

- **MPPE (Microsoft Point-to-Point Encryption).** כל חיבורי PPP, כולל PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol), אך לא כולל L2TP (**L**ayer **2 T**unneling **P**rotocol), יכולים להשתמש ב-MPPE. MPPE משתמשת בהצפנה מסוג Rivest-Shamir-Adleman (RSA) Rivest's Cypher 4 (RC4) Stream Cypher, ונעשה בה שימוש רק כאשר נעשה שימוש בשיטות האימות EAP-Transport Layer Security (TLS) או MS-CHAP (גירסה 1 או 2). MPPE יכולה להשתמש במפתחות הצפנה באורך של 40, 56 ו-128 סיביות. המפתח באורך 40 סיביות (40-bit Encryption Key) נועד לשם תאימות לאחור ולשימוש בינלאומי. המפתח באורך 56 סיביות נועד לשימוש בינלאומי, ועומד במגבלות חוקי הייצוא של ארה"ב. המפתח באורך 128 סיביות נועד לשימוש בצפון אמריקה. כברירת מחדל, בעת תהליך הקמת החיבור נערך משא ומתן לגבי אורך המפתח הגדול ביותר הנתמך על ידי הנתב המתקשר והנתב העונה. אם לצד העונה נדרש מפתח הצפנה ארוך יותר מזה הנתמך על ידי הצד המתקשר, יידחה ניסיון ההתחברות.

הערה לחיבורי רישות בחיוג (Dial-up Networking) Windows 2000 משתמשת ב-MPPE.

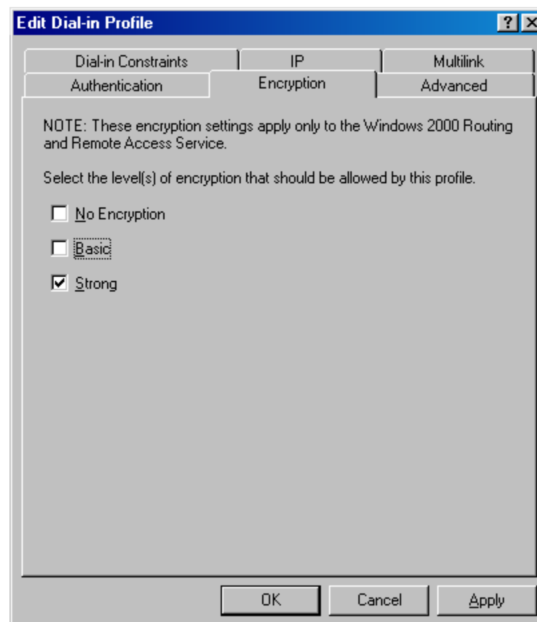
הערת המתרגם למרות האמור בפיסקה האחרונה, הממשל האמריקאי אישר למדינות רבות, וביניהן ישראל, להשתמש במפתח הצפנה באורך 128 סיביות. עדכון למפתח ההצפנה ניתן להורדה באופן חופשי מאתר האינטרנט של Microsoft. הפיסקה תורגמה כפי שהיא מופיעה בספר המקורי כדי להיות תואמת לבחינה, במידה ותישאל שאלה בנושא.

- **IPSec (IP Security).** לחיבורי חיוג-על-פי-דרישה (Demand-Dial) המשתמשים ב-L2TP over IPSec, נקבעת ההצפנה על ידי הקמת SA (**S**ecurity **A**ssociation) של IPSec. אלגוריתמי ההצפנה הזמינים כוללים DES (**D**ata **E**ncryption **S**tandard) עם מפתח באורך 56 סיביות, ו-DES משולש (Triple DES, 3DES) העושה שימוש בשלושה מפתחות באורך 56 סיביות ונועד לסביבות הדורשות רמת אבטחה גבוהה במיוחד. מפתחות ההצפנה הראשוניים נגזרים מתוך תהליך האימות של IPSec.

עבור חיבורי VPN משתמשת Windows 2000 ב-MPPE עם PPTP ובהצפנת IPSec עם L2TP.

כדי להגדיר הצפנה עבור חיבורי חיוג

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ובחר Routing and Remote Access.
2. תחת שם השרת לחץ על Remote Access Policies.
3. בחלונית הפרטים לחץ לחיצה ימנית על מדיניות הגישה מרחוק אותה אתה מעוניין להגדיר, ומתפריט הקיצור בחר Properties.
4. לחץ על Edit Profile.
5. בחר בכרטיסיה Encryption, המוצגת בתרשים 14.4, קבע הגדרות לפי הצורך, ולסיום לחץ OK.
6. לחץ OK כדי לסגור את תיבת דו-שיח Policy Properties.



תרשים 14.4 הגדרת רמת ההצפנה

סיכום שיעור

גישה מרחוק מאפשרת ללקוחות להתחבר לרשת שלך ממיקום מרוחק באמצעות התקני חומרה שונים, הכוללים כרטיסי רשת ומודמים. לאחר שהלקוח יצר חיבור בגישה מרחוק הוא יכול להשתמש במשאבי הרשת, כגון קבצים, ממש אילו היה מחובר ישירות לרשת המקומית. ב- Windows 2000 אתה יוצר מדיניות גישה מרחוק ואז מגדיר את האבטחה לגביהן. ניתן להגדיר את רמת ההצפנה עבור חיבורי גישה מרחוק בחיוג.

שיעור 3: ניטור אירועי אבטחה

בשיעור 1 למדת אודות החלקים השונים של תוכנית אבטחת הרשת. מדיניות מנהלתיות לתוכנית האבטחה כוללות מדיניות להאצלת סמכות על משימות ניהוליות וניטור יומני ביקורת, כדי לזהות פעילות חשודה. בשיעור זה תלמד כיצד לנטר אירועי אבטחה בסביבת Windows 2000, כדי למנוע התקפות ופריצות לרשת שלך.

לאחר שיעור זה, תוכל

- לנהל ולנטר תעבורת רשת.
- לנהל ולנטר גישה מרחוק.

זמן לימוד משוער: 45 דקות

ניטור אבטחת הרשת

טכנולוגיות אבטחת הרשת אותן תיישם, כגון Microsoft Proxy Server, עשויות להתאים למטרות האבטחה שלך, אם אתה מתכנן בקפידה את הגדרותיהן. כאשר ההכנה המוקדמת טובה מספיק, יכולה פעולה זו להתבצע בהצלחה גדולה. אבל, צפיית כל שיקולי האבטחה מראש היא דרישה מכבידה עד מאוד, מפני ש:

❖ מתפתחים סיכונים חדשים.

❖ מערכות יכולות להתקלקל והסביבה בה ממוקמים המחשבים שלך משתנה במשך הזמן.

על ידי מעקב מתמיד אחר אסטרטגיות האבטחה של הרשת שלך תוכל למזער את סיכוני האבטחה. אבל, עליך גם לצפות בפעילות האבטחה המתבצעת בפועל, כדי לאתר נקודות תורפה לפני שהן ינוצלו, וכדי לעצור ניסיונות חדירה לפני שהם ישפיעו על הרשת.

כדי לצפות בפעילות האבטחה של הרשת דרושים לך כלים ללכידת נתוני הפעילות ולניתוח הנתונים הנלכדים. לדוגמה, Microsoft Proxy Server כולל ניהול יומנים בשתי רמות: Normal ו- Verbose. Windows 2000 עצמה כוללת גם יומן לרישום אירועים, אותו ניתן להרחיב על ידי אפשור רישום אירועי אבטחה. IAS, הנדון בשלב מאוחר יותר של פרק זה, כולל מיגוון רחב של אפשרויות דיווח פעילויות. כדי לסייע בניטור שרתים ויישומים, כולל שרתי אבטחה ויישומים, ניתן למצוא גם מוצרים של צד-שלישי.

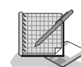
הערה כאשר אתה משתמש בשרתי אבטחה ויישומים, סקור בקפידה את תיעוד המערכות בהן אתה משתמש ובחר את אפשרויות רישום היומן התואמות לצרכיך.

שימוש ב- Event Viewer לניטור אבטחה

Event Viewer (צופה האירועים) מאפשר לך לנטר (Monitor) אירועים במערכת שלך. הוא שומר דוחות לגבי תוכניות, אבטחה ואירועי מערכת במחשב שלך. תוכל להיעזר ב- Event Viewer כדי לצפות ולנהל את יומני האירועים, לאסוף מידע אודות תקלות חומרה או תוכנה, ולסקור את אירועי האבטחה של Windows 2000. השירות Event Log מופעל באופן אוטומטי בעת הפעלת Windows 2000. כל המשתמשים יכולים לצפות באירועי מערכת ובאירועי יישומים. תוכל גם להגדיר את מערכת ההפעלה Windows, כך שתבקר (Audit) גישה למשאבים מסוימים, וכי אלה יירשמו ביומן האבטחה (Security Log). טבלה 14.4 מציגה מיגוון אירועים אותם תוכל לבקר, כמו גם את סיכון האבטחה המסוים אותו מנטרת תוכנית הבקרה.

טבלה 14.4 תכונות האבטחה של Windows 2000

אירוע מבוקר	סכנה שאותרה
בקרה כושלת של כניסה/יציאה מהמערכת	ניסיון פריצה עם סיסמה מזדמנת
בקרה מוצלחת של כניסה/יציאה מהמערכת	פריצה עם סיסמה גנובה
בקרה מוצלחת של זכויות משתמש, ניהול משתמש וקבוצה, שינויים באבטחה במדיניות, אתחול מחדש, כיבוי ואירועי מערכת	שימוש לא כשר בזכויות
בקרה מוצלחת/כושלת של אירועי גישה לקבצים ולאובייקטים. בקרה מוצלחת של File Manager בגישה לקריאה/כתיבה רגישים על ידי משתמשים או קבוצות חשודים	גישה לא מורשית לקבצים רגישים
בקרה מוצלחת/כושלת של אירועי גישה לקבצים מדפסות ולאובייקטים. בקרה מוצלחת/כושלת של Print Manager בגישה למדפסות על ידי משתמשים או קבוצות חשודים	גישה לא מורשית למדפסות
בקרה מוצלחת/כושלת של אירועי כתיבה לקבצי תוכניות (exe או dll). בקרה מוצלחת או כושלת של מעקב אחרי הליכים. הפעל את התוכניות החשודות; בדוק את יומן האבטחה לאיתור ניסיונות לא צפויים לשינוי קבצי תוכניות או יצירת הליכים לא צפויים. הפעל רק כאשר אתה מנטר בפועל את יומן המערכת	התפרצות וירוס



תרגול: רישום נסיונות כושלים לכניסה למערכת

ביקורת אבטחה (Security Auditing) אינה מופעלת כברירת מחדל. עליך להפעיל את סוגי הביקורת המבוקשים על ידך תוך שימוש ביישום Group Policy, שהוא יישום Snap-In של MMC. בנוסף, עליך גם לאפשר ביקורת עבור אזורים כלליים או עבור פריטים ספציפיים, אחריהם אתה מעוניין לעקוב.

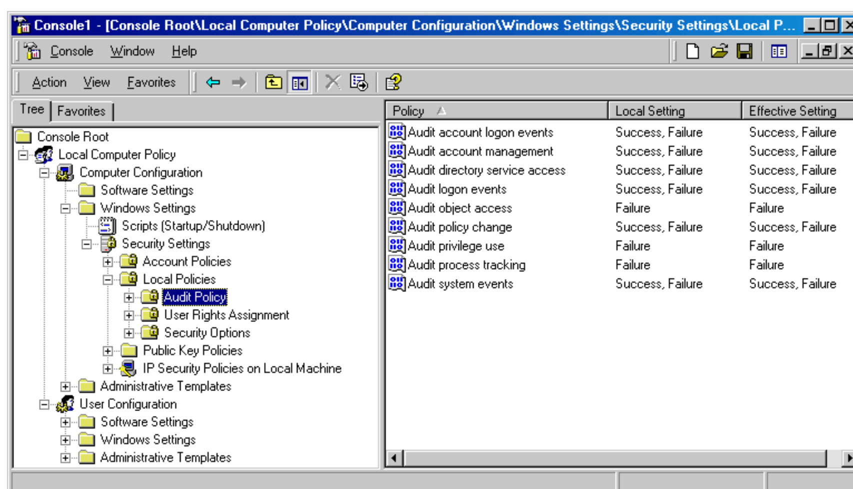
➢ כדי להפעיל ביקורת אחר ניסיונות כושלים לכניסה למערכת

1. לחץ Start, בחר Run, הקלד mmc, ולחץ OK.
2. פתח את תפריט Console, לחץ על Add/Remove Snap-In, ולחץ Add.
מופיעה תיבת דו-שיח Add/Remove Snap-In.
3. לחץ Add.
מופיעה תיבת דו-שיח Add Standalone Snap-In.
4. בחר Group Policy, ולחץ Add.
מופיעה תיבת דו-שיח Select Group Policy.
5. לחץ על Finish כדי להוסיף את המחשב המקומי.
תוכל גם ללחוץ על Browse ואז לבחור מחשב אחר ברשת שלך.
6. בתיבת דו-שיח Add Standalone Snap-In לחץ על Close.
7. בתיבת דו-שיח Add/Remove Snap-In לחץ על OK.
8. עקוב אחר הנתיב בעץ:

Local Computer Policy/Computer Configuration/Windows Settings/Security Settings/ Local Policies

לחץ על Audit Policy, כפי שמופיע בתרשים 14.5.

9. בחלונית הפרטים לחץ לחיצה ימנית על Audit Logon Events ואז לחיצה ימנית על Security.
מופיעה תיבת דו-שיח Local Security Policy Settings.
10. תחת Audit These Attampts, בחר Failure, ולחץ OK.



תרשים 14.5 בחירת מדיניות ביקורת עבור מדיניות המחשב המקומי

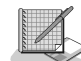
צפייה ביומן אירועי האבטחה

אתה יכול לקבוע שרשומת ביקורת תירשם ליומן אירועי האבטחה בכל פעם שפעולות מסוימות מבוצעות, או כאשר מתבצעת גישה לקבצים מסוימים. רשומת ביקורת מציגה את הפעולה שבוצעה, המשתמש שביצע אותה ואת התאריך והשעה בה בוצעה הפעולה. תוכל לבקר גם הצלחות וגם כשלים של ביצוע פעולה, כך שעקבות הביקורת יכולים לספר לך מי ביצע פעולות ברשת ומי ניסה לבצע פעולות שאינן מורשות. תוכל לצפות ביומן האירועים באמצעות Event Viewer.

רישום אירועי אבטחה הוא סוג מסויים של איתור פריצה למחשב באמצעות ביקורת. ביצוע הביקורת ורישום יומני אבטחה של הרשת הם אמצעי אבטחה חשובים מאוד. Windows 2000 מאפשרת לך לנטר מיגוון רחב של אירועים, אשר יכולים לשמש למעקב אחר פעולותיו של פולש.

יומן האבטחה (Security Log) רושם אירועי אבטחה, כגון ניסיונות כניסה חוקיים ושאינם חוקיים למערכת, ואירועים הקשורים בשימוש במשאבים, כגון יצירת, פתיחת או מחיקת קבצים או אובייקטים אחרים. יומן האבטחה מסייע לעקוב אחר שינויים למערכת האבטחה ומזהה "חורי" אבטחה (Security Breaches) אפשריים. לדוגמה, ניסיון להיכנס למערכת עשוי להירשם ביומן האבטחה, אם האפשרויות לביקורת פעולות כגון Logon ו-Logoff מאופשרת. אם יומן האבטחה נבדק באופן סדיר ולעיתים תכופות, יקל הדבר על זיהוי חלק מסוגי ההתקפה, כגון מתקפת ססמאות, לפני שיצליח הדבר בידי מבצעו. לאחר החדירה, יכול יומן האבטחה לסייע לך לקבוע כיצד חדר הפולש למערכת ומה הוא או היא עשו בה. רשומות קובץ יומן האבטחה משמשות כראייה משפטית חוקית וקבילה לאחר שהפולש זוהה.

הערה כדי לשמר את רמת האבטחה הגבוהה ביותר, בדוק את יומני האבטחה לעיתים תכופות.

 תרגול: צפייה ביומן אירועי אבטחה

יומני אירועים כוללים כותרת, תיאור האירוע (בהתבסס על סוג האירוע) ואפשר גם שיכללו נתונים נוספים. רוב רשומות יומני האבטחה כוללים כותרת ותיאור. Event Viewer מציג את האירועים מכל יומן באופן נפרד. כל שורה מציגה מידע אודות אירוע יחיד, וכוללת תאריך, שעה, מקור, סוג האירוע, קטגוריה, מזהה אירוע, חשבון משתמש ושם המחשב. בתרגול זה תסקור את יומן אירועי האבטחה כדי לזהות ניסיון חדירה לא מאושר לרשת. כדי להשלים תרגול זה, עליך לבצע את הצעדים שבתרגול הקודם של שיעור זה.

➢ **כדי לצפות ביומן אירועי האבטחה (Security Event Log)**

1. נסה להיכנס למחשב Windows 2000 בו הפעלת את ביקורת האבטחה עבור ניסיונות כניסה כושלים, תוך שימוש בשם משתמש וסיסמה לא חוקיים במערכת.

2. לאחר כישלון הכניסה, הקלד שם משתמש וסיסמה חוקיים והיכנס למערכת.

3. לחץ Start, הצבע על Program, Administrative Tool, ובחר את Event Viewer.

מופיע חלון Event Viewer.

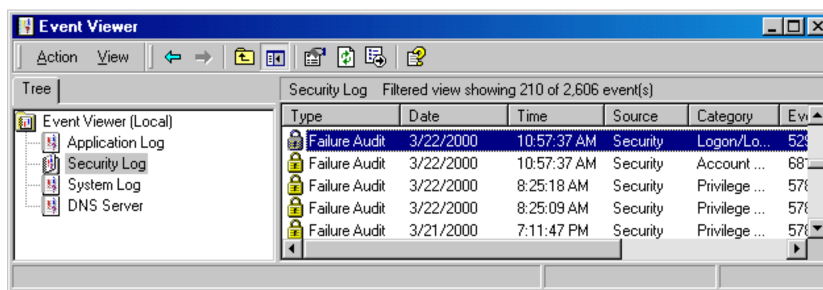
4. בחלונית השמאלית לחץ על Security Log.

שים לב שניסיונות הכניסה הלא חוקיים מוצגים בחלונית הימנית של Event Viewer, כפי שניתן לראות בתרשים 14.6.

5. לחץ לחיצה כפולה על הפריט Failure Audit שבתצוגת האירועים, כדי לפתוח את החלון Event Properties.

שים לב לחלק התיאור, אשר מתאר בפניך את הסיבה לכשל ואת שם המשתמש שהקלדת, אך לא את הסיסמה שהקלדת.

6. לחץ OK כדי לסגור את חלון Event Properties.



תרשים 14.6 רשומת ניסיון כניסה לא חוקי ביומן אירועי האבטחה

System Monitor

System Monitor הוא כלי אשר יכול לשמש למעקב אחר ניצולת משאבי המערכת. הוא יכול לשמש לבחינת כמות משאבי המערכת המנוצלים על ידי יישום מסוים. אובייקטים שכיחים אותם יכול המשתמש לרשום ביומן, הם זיכרון, מעבד, רשת ופעילות דיסק. מונים נוספים, למרות שאין בינם לבין ביצועי המערכת כל קשר, מספקים מידע יעיל אודות אבטחת השרת. אלה כוללים את :

- ❖ Server/Errors Access Permissions
- ❖ Server/Errors Granted Access
- ❖ Server/Errors Logon
- ❖ IIS Security

➢ כדי לנטר אירועי אבטחה באמצעות System Monitor

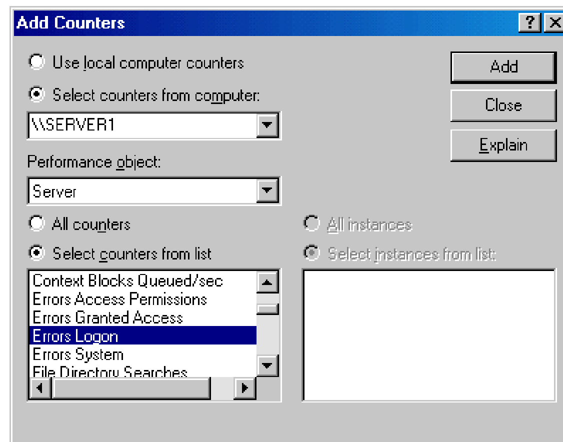
1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ובחר Performance.

נפתח MMC ובו System Monitor.

2. בחלונית הימנית לחץ על Add.

מופיעה תיבת דו-שיח Add Counters, כפי שמוצג בתרשים 14.7.

3. מתיבת הרשימה הנפתחת Performance Object בחר Server.
4. לחץ על לחצן האפשרויות Select Counters From List.
5. מרשימת המונים בחר מונה, ולחץ על Add.
6. לחץ Close כדי לסגור את תיבת דו-שיח Add Counters.



תרשים 14.7 הוספת המונה Error Logon

תוכנית השירות IPSec Monitor

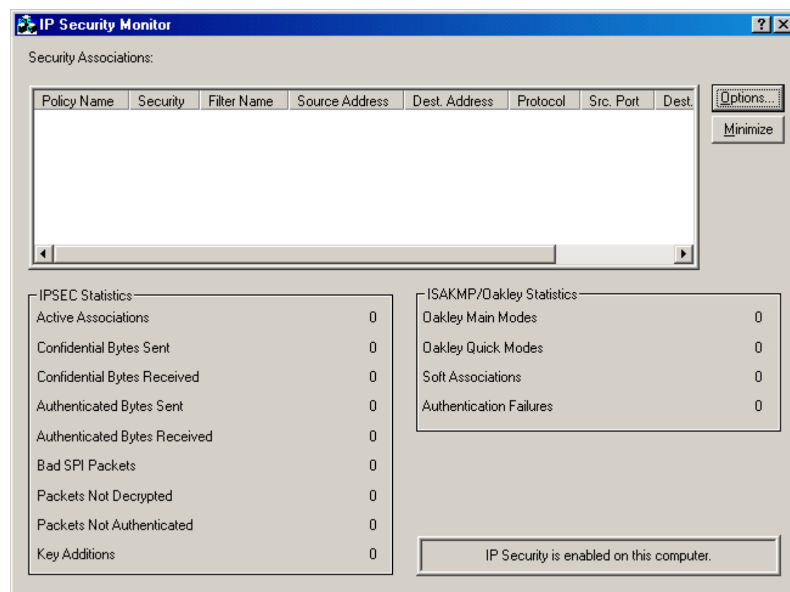
IPSec Monitor יכול לאמת האם ההתקשרויות המאובטחות שלך מוצלחות, על ידי הצגת ה-SA הפעיל במחשב מקומי או מרוחק. לדוגמה, תוכל להיעזר ב- IPSec Monitor כדי לקבוע האם קיימת תבנית של כשלים באימות או כשלים של SAs, דבר שיכול להצביע על הגדרות מדיניות אבטחה שאינן תואמות. IPSec Monitor יכול להיות מופעל במחשב המקומי או שניתן להפעילו מרחוק, אם יש לך חיבור רשת למחשב המרוחק.

➢ כדי להפעיל את IPSec Monitor

1. לחץ Start, ולחץ Run.
2. בתיבת הטקסט Open שבתיבת דו-שיח Run הקלד את הפקודה <computername> ipsecmon, ולחץ על OK.

נפתחת תיבת דו-שיח IP Security Monitor, כפי שנראית בתרשים 14.8. עבור כל SA פעיל מופיעה רשומה. המידע המופיע בכל רשומה כולל את שם מדיניות IPSec הפעילה, את Filter Action ו- IP Filter List (כולל פרטים אודות המסנן הפעיל הפעילים ואת נקודת הקצה הסופית של התעלה (אם כזו הוגדרה).

3. לחץ Options כדי להגדיר קצב רענון.



תרשים 14.8 ממשק IP Security Monitor

IPSec Monitor יכול גם לספק סיוע בכיוונון עדין ובאיתור תקלות, כולל הסטטיסטיקות הבאות:

- ❖ מספר וסוג SAs הפעילים.
- ❖ מספרם הכולל של מפתחות שיח (Session Keys) ומפתחות מאסטר (Master Keys). SA מוצלח של IPSec גורם בראשיתו ליצירת מפתח מאסטר אחד ומפתח שיח אחד. יצירת מפתחות עוקבים מוצגים כמפתחות שיח נוספים.
- ❖ מספרם הכולל של בתים (Bytes) סודיים (Confidential, Encapsulated Security Payload) או מאומתים (Authenticated, Encapsulated Security Payload או כותרות מאומתות) הנשלחים או מתקבלים.

ניטור תקורת האבטחה

אבטחה מושגת רק על חשבון פגיעה מסוימת בביצועים. מדידת תקורת הביצועים של אסטרטגיית אבטחה היא אינה פעולה פשוטה של ניטור הליך (Process) או מטלה (Thread). התכונות של מודל האבטחה של Windows 2000 ושירותי אבטחה אחרים משולבים לתוך מספר שירותים שונים של מערכת ההפעלה. אינך יכול לנטר את תכונות האבטחה בנפרד מהשירותים האחרים. במקום זאת, הדרך השכיחה ביותר למדידת תקורת האבטחה היא להפעיל בדיקות המשוות את ביצועי השרת עם ובלי תכונות אבטחה פעילות. ניתן להפעיל את הבדיקות עם עומס עבודה קבוע ותצורת שרת קבועה, כך שתכונות האבטחה הן המשתנה היחיד.

בעת הבדיקות תוכל לבדוק:

- פעילות המעבד (Processor Activity) ותור המעבד (Processor Queue)
- שימוש בזיכרון פיסי (Physical Memory Used)
- תעבורת רשת (Network Traffic)
- זמן אחזור (Latency) ועיכובים (Delays)

סיכום שיעור

עליך לנטר את פעילות האבטחה ברשת כדי לזהות את נקודות התורפה, לפני שניתן יהיה לנצל אותן. תוכל להיעזר ב- Event Viewer כדי לצפות ולנהל את אירועי האבטחה של Windows 2000. רשומת ביקורת (Audit Entry) מציגה את הפעולה שבוצעה, המשתמש שביצע אותה, ואת התאריך והשעה בה בוצעה הפעולה. הן System Monitor והן Network Monitor יכולים לספק מידע חשוב לגבי אבטחת השרת. IPSec Monitor יכול לוודא האם התקשורת המאובטחת שלך מוצלחת. בנוסף, תוכל להיעזר ב- Routing and Remote Access כדי לנטר תעבורת גישה מרחוק ב- Windows 2000, ולאפשר יצירת יומן כדי לסקור מידע זה.

שאלות סיכום

השאלות הבאות נועדו לחזק את הנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות על שאלה, עיין בשיעור המתאים ונסה את השאלה שנית. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואחר כך בעברית.

Answering the following questions will reinforce key information presented in this chapter. If you are unable to answer a question, review the appropriate lesson and then try the question again. Answers to the questions can be found in Appendix A, "Questions and Answers".

1. What are some potential security risks you should identify in your security plan?
2. What is authentication and how can you implement it?
3. What are some security features of Windows 2000?
4. How can you secure a connection between your network and the Internet?
5. What are some remote access protocols you can implement for security?
6. Name two forms of encryption available for demand-dial connections.
7. How do System Monitor and Network Monitor provide the ability to monitor security on your network?
8. How is Event Viewer used to monitor security?
9. How do you enable remote access logging in Windows 2000?

1. מהם חלק מסיכוני האבטחה שעליך לזהות בתוכנית האבטחה שאתה יוצר?
2. מהו אימות, וכיצד עליך ליישם אותו?
3. מנה חלק מתכונות האבטחה של Windows 2000.
4. כיצד ניתן לאבטח חיבור בין הרשת שלך ורשת האינטרנט?
5. מנה חלק מהפרוטוקולים לגישה מרחוק אותם תוכל ליישם לצרכי אבטחה.
6. מנה שני אופני הצפנה הזמינים לחיבוריות בחיוג-בדרישה.
7. כיצד מספקים System Monitor ו- Network Monitor את האפשרות לנטר אבטחה ברשת שלך?
8. כיצד ניתן להשתמש ב- Event Viewer לניטור אבטחה?
9. כיצד אתה מאפשר ניהול יומן גישה מרחוק ב- Windows 2000?

נספחים

חלק זה כולל:

- נספח שאלות ותשובות באנגלית
- מילון מונחים (Glossary) באנגלית
- אינדקס באנגלית.

שים לב, הנספח הראשון מתחיל בעמוד 1 שנמצא בסוף הספר (לפני הקטלוג המצורף), ומתקדם משמאל לימין לתוך הספר.

Microsoft Windows© 2000

Network Infrastructure Administration

- גירסה אלקטרונית מלאה של הספר באנגלית,
- קטעי לימוד בוידאו,
- קטלוג ספרי הוד-עמי.

© Microsoft Corporation.
All Rights Reserved.

התוכנה מופצת AS IS
ללא תמיכה כלשהי.

הוראות התקנה:
הכנס/י את התקליטור לכונן התקליטורים. קרא/י קובץ OnCD.

התקליטור מופץ על ידי

הוצאת הוד-עמי לספרי מחשבים

כבונוס ללקוחותיה

www.**hod-ami**.co.il

09-9564716

כל הזכויות שמורות לחברת Microsoft. אזהרה: העתקה בלתי חוקית של תקליטור זה או חלק ממנו מהווה עבירה פלילית. היישומים המופיעים בתקליטור זה מסופקים באחריות חברת Microsoft המייצרת אותם. הוצאת הוד-עמי אינה אחראית, בכל צורה שהיא, לאופן ולטיב התוכנות המותקנות.

Appendix A

Questions and Answers

Chapter 1

Review Questions

1. You are currently configuring TCP/IP manually for new computers and computers moving from one subnet to another. You want to simplify management of TCP/IP addresses and assign them automatically. Which Windows 2000 network service should you use?

   Use DHCP to automate and centrally manage TCP/IP addresses.

2. You have an Alpha server with 8 GB of RAM and 8 CPUs. You want to provide file services to over 400 people in your company. Which Windows 2000 operating system would be most appropriate to deploy, and why?

   In this case, deploy Windows 2000 Advanced Server because it provides network load balancing and enterprise memory architecture. Windows 2000 Server only supports 2 GB of RAM, so it would not satisfy the necessary requirements.

3. You want a Windows 2000 server to connect to and provide routing for AppleTalk-based Macintosh networks. What protocol should you install?

   Windows 2000 supports an AppleTalk protocol stack and AppleTalk routing software so that the Windows 2000 server can connect to and provide routing for AppleTalk-based Macintosh networks.

Chapter 2

Review Questions

1. What is TCP/IP?

   TCP/IP is a suite of protocols that provide routing in WANs, and connectivity to a variety of hosts on the Internet.

2. Which TCP/IP utilities are used to verify and test a TCP/IP configuration?

   PING and Ipconfig.

3. What is the purpose of a subnet mask?

   To mask a portion of the IP address so IP can distinguish the network ID from the host ID.

4. What is the minimum number of areas in an OSPF internetwork?

   An OSPF internetwork always has at least one area called the backbone, whether or not it is subdivided into areas.

5. What is an internal router?

   An internal router is a router with all interfaces connected to the same area.

6. What is a border router?

   A border router, or ABR, is a router with interfaces connected to different areas.

7. What Windows 2000 administrative tool can you use to manage internal and border routers?

   Routing and Remote Access.

Chapter 3

Review Questions

1. What is NWLink and how does it relate to Windows 2000?

   NWLink is the Microsoft implementation of IPX/SPX. You must use this protocol if you want to use Gateway Service for NetWare or Client Service for NetWare to connect to NetWare servers.

2. What is SPX?

   SPX is a transport protocol that offers connection-oriented services over IPX. SPX is used by utilities that require a continuous connection, and provides reliable delivery using sequencing and acknowledgments and verifies successful packet delivery to any network destination by requesting verification from the destination on receipt of the data. SPX also provides a packet burst mechanism that allows the transfer of multiple data packets without requiring that each packet be sequenced and acknowledged individually.

3. What is Gateway Service for NetWare?

   Gateway Service for NetWare allows you to create a gateway through which Microsoft client computers without Novell NetWare client software can access NetWare file and print resources.

4. When choosing between using Client Service for NetWare and Gateway Service for NetWare, what should you consider?

   If you intend to create or indefinitely maintain a heterogeneous environment composed of both servers running Windows 2000 and servers running NetWare, consider using Client Service for NetWare. If you intend to migrate gradually from NetWare to Windows 2000 or if you want to reduce administration, consider using Gateway Service for NetWare.

5. What is the NWLink Auto Detect feature?

   The Windows 2000 NWLink Auto Detect feature detects the frame type and network number that are configured on NetWare server(s) on the same network. NWLink Auto Detect is the recommended option for configuring both the network number and the frame type. If the Auto Detect feature selects an inappropriate frame type and network number for a particular adapter, you can manually reset an NWLink frame type or network number for that given adapter.

Chapter 4

Review Questions

1. What is the purpose of analyzing frames with Network Monitor?

   Analyzing frames allows you to identify client-to-server connection problems, find a computer that makes a disproportionate number of requests, and isolate Application Layer problems.

2. What kind of data does a frame contain?

   Each frame contains the source address of the computer that sent the message, the destination address of the computer that the frame was sent to, headers from each protocol used within the frame, and the payload being sent.

3. What is a capture filter, and what is it used for?

   A capture filter functions like a database query. You can use it to specify the types of network information you want to monitor. For example, to see only a specific subset of computers or protocols, you can create an address database, use the database to add addresses to your filter, and then save the filter to a file. By filtering frames, you save both buffer resources and analysis time. Later, if necessary, you can load the capture filter file and use the filter again.

Chapter 5

Practice Questions

Lesson 3: Customizing IPSec Policies and Rules Practice: Building a Custom IPSec Policy

At this point, you still have not configured your custom rule. Only the default response rule properties have been configured. What is the purpose of the default response rule?

The default response rule enables negotiation with computers requesting IPSec. A default response rule is added to each new policy you create, but it is not automatically activated. A default response rule can be used for any computer that does not require security, but must be able to appropriately respond when another computer requests secured communications. It can also be used as a template for defining custom rules.

Review Questions

1. IPSec is defined by what standards group?

   The Internet Engineering Task Force (IETF) IP Security working group.

2. Define the difference between secret and public key cryptography.

   Secret key cryptography uses a single preshared key. Public key cryptography uses a key pair, one for encrypting data and verifying digital signatures and the second for decrypting data and creating digital signatures.

3. ISAKMP/Oakley provides what functionality?

   ISAKMP/Oakley establishes a secure channel between two computers for communication and establishes an SA.

4. What are rules comprised of?

   Rules are comprised of IP filters, negotiation policies, authentication methods, IP tunneling attributes, and adapter types.

5. When would a public key certificate be used?

   A public key certificate allows a nontrusted domain computer to use IPSec to communicate with a trusted domain computer.

6. What is an IP filter used for?

   IP filters check datagrams for a match against each filter specification. This allows for filtering based on the source and destination address, DNS name, protocol, or protocol ports.

Chapter 6

Practice Questions

Lesson 3: The Hosts File Practice: Working with the Hosts File and DNS

➢ To ping your local host name

1. Type **ping Server1** (where Server1 is the name of your computer) and then press the Enter key. What was the response?

   Four successful "Reply from IP address" messages.

➢ To ping a local computer name

1. Type **ping computertwo** and then press the Enter key. What was the response?

   "Bad IP address computertwo."

➢ To use the HOSTS file for name resolution

1. Type **ping computertwo** and then press the Enter key. What was the response?

   Four successful "Reply from IP address" messages.

Review Questions

1. What is a host name?

   An alias assigned to a TCP/IP host for the purpose of simplifying access to the host.

2. What is the purpose of a host name?

   To simplify how a host is referenced. Host names are used with PING and other TCP/IP applications.

3. What does a Hosts file entry consist of?

   The host name or names and the corresponding IP address.

4. During the name resolution process, what occurs first: ARP resolution or host name resolution?

   Host name resolution.

Chapter 7

Practice Questions

Lesson 3: Planning a DNS Implementation

Scenario 1: Designing DNS for a Small Network

1. How many DNS domains will you need to configure?

   One (or zero, if they have an ISP to manage the name server).

2. How many subdomains will you need to configure?

   Zero.

3. How many zones will you need to configure?

   One (or zero, if they have an ISP to manage the name server).

4. How many primary name servers will you need to configure?

   One (or zero, if they have an ISP to manage the name server).

5. How many secondary name servers will you need to configure?

   One (or zero, if they have an ISP to manage the name server).

6. How many DNS cache-only servers will you need to configure?

   Zero.

Scenario 2: Designing DNS for a Medium-Size Network

1. How many DNS domains will you need to configure?

   You will need at least one DNS domain that can contain both hosts (computers or services) and subdomains.

2. How many subdomains will you need to configure?

   Three. Your DNS domain includes multiple sites, so you should subdivide the domain to create three subdomains that reflect these groupings.

3. How many zones will you need to configure?

   Four. You can distribute administrative tasks to different groups in the primary sites by configuring four zones. This will also provide more efficient data distribution.

4. How many primary name servers will you need to configure?

   Four. Primary sites will maintain their own equipment and the equipment of the branch offices connected to them. Therefore, you must configure four primary name servers.

5. How many secondary name servers will you need to configure?

   Branch offices have between 25 and 250 users needing access to all four of the primary sites. When a secondary server is configured for a zone, clients can still resolve names for that zone even if the primary server for the zone goes down; therefore, you should configure four secondary name servers.

6. How many DNS cache-only servers will you need to configure?

   You should configure 10 cache-only servers (one per branch office). This will speed the performance of DNS resolution, reduce DNS-related query traffic, and improve reliability.

7. Use the following mileage chart to design a zone/branch office configuration based on the geographical proximity between each primary site and branch office. Branch offices should be in the same zone as the nearest primary site.

   Zones for each branch office (based on geographical proximity):

Portland, OR	Atlanta	Boston	Chicago
Los Angeles	Montreal	Denver	Dallas
Salt Lake City	Washington, DC	Kansas City	Miami
San Francisco			New Orleans

Mileage Chart	Atlanta	Boston	Chicago	Portland, OR
Dallas	807	1817	934	2110
Denver	1400	1987	1014	1300
Kansas City	809	1454	497	1800
Los Angeles	2195	3050	2093	1143
Miami	665	1540	1358	3300
Montreal	1232	322	846	2695
New Orleans	494	1534	927	2508
Salt Lake City	1902	2403	1429	800
San Francisco	2525	3162	2,187	700
Washington, DC	632	435	685	2700

Scenario 3: Designing DNS for a Large Network

1. How many DNS domains will you need to configure?

   Zero (the domain for this company is in Geneva, Switzerland).

2. How many subdomains will you need to configure?

   Eleven. Remember that you want to give control of the equipment to each subsidiary, and to have a resource domain in each subsidiary.

3. How many zones will you need to configure?

   Each of the regional headquarters' subsidiaries will maintain total control of users within their areas. Therefore, you should configure 11 zones.

4. How many primary name servers will you need to configure?

   One of the requirements defined in this scenario is that line of business applications running on your computers will be configured as servers within the domains. Therefore, you should configure 11 primary name servers.

5. How many secondary name servers will you need to configure?

   You can configure servers to host as many different primary or secondary zones as is practical. In this case, line of business applications need to be available to all sites within their areas, as well as the other regional head-quarters. Therefore, you should configure 11 secondary name servers for redundancy. When a secondary server is configured for a zone, clients can still resolve names for that zone even if the primary server for the zone goes down.

6. How many DNS cache-only servers will you need to configure?

   Three or more. At least one per regional headquarter.

Review Questions

1. Name the three components of the DNS.

   Resolver, name servers, and domain name space.

2. Describe the differences among primary, secondary, and master name servers.

   A primary name server has zone information in locally maintained zone files. A secondary name server downloads zone information. A master name server is the source of the downloads for a secondary name server (which could be a primary or secondary name server).

3. List three reasons to have a secondary name server.

   - **It operates as a redundant name server (you should have at least one redundant name server for each zone).**
   - **If you have clients in remote locations, you should have a secondary name server to avoid communicating across slow links.**
   - **A secondary name server reduces the load on the primary name server.**

4. Describe the difference between a domain and a zone.

   A domain is a branch of the DNS name space. A zone is a portion of a domain that exists as a separate file on the disk storing resource records.

5. Describe the difference between recursive and iterative queries.

   In a recursive query, the client instructs the DNS server to respond with either the requested information or an error that the information was not found. In an iterative query, the DNS server responds with the best answer it has, typically a referral to another name server that can help resolve the request.

6. List the files required for a Windows 2000 DNS implementation.

   Database file, cache file, and reverse lookup file.

7. Describe the purpose of the boot file.

   The boot file is used in the Berkeley Internet Name Daemon implementation to start up and configure the DNS server.

Chapter 8

Review Questions

1. How many zones can a single DNS server host?

   A single DNS server can be configured to host zero, one, or multiple zones.

2. What benefits do DNS clients obtain from the dynamic update feature of Windows 2000?

   Dynamic update enables DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur. This reduces the need for manual administration of zone records, especially for clients that frequently move or change locations and use DHCP to obtain an IP address.

3. Name one benefit and one disadvantage of a caching-only server.

   The benefit provided by caching-only servers is that they do not generate zone transfer network traffic because they do not contain any zones. A disadvantage of a caching-only server is that when the server is initially started, it has no cached information and must build up this information over time as it services requests.

4. List and describe three DNS performance counters.

   - **Dynamic update and secure dynamic update counters, for measuring registration and update activity generated by dynamic clients.**
   - **Memory usage counters, for measuring system memory usage and memory allocation patterns created by operating the server computer as a Windows 2000 DNS server.**
   - **Recursive lookup counters, for measuring queries and responses when the DNS Server service uses recursion to look up and fully resolve DNS names on behalf of requesting clients.**

Chapter 9

Review Questions

1. What are two benefits of WINS?

   - **Automatic name registration and resolution of NetBIOS names**
   - **Provides internetwork and interdomain browsing**
   - **Eliminates the need for a local LMHOSTS file**

2. What two methods can be used to enable WINS on a client computer?

   Manual and automatic with DHCP.

3. How many WINS servers are required in an intranet of 12 subnets?

   Only one is required. It is recommended to have multiple servers for redundancy.

4. What types of names are stored in the WINS database?

   NetBIOS unique and group names.

Chapter 10

Review Questions

1. What is DHCP?

   Dynamic Host Configuration Protocol simplifies the administrative management of IP address configuration by automating address configuration for network clients.

2. Describe the integration of DHCP with DNS.

   A DHCP server can enable dynamic updates in the DNS name space for any DHCP clients that support these updates. Scope clients can then use DNS with dynamic updates to update their computer name-to-IP address mapping information whenever changes occur to their DHCP-assigned address.

3. What is a DHCP client?

   The term client is used to describe a networked computer that requests and uses the DHCP services offered by a DHCP server.

4. What is IP autoconfiguration in Windows 2000?

   Windows 2000-based clients can automatically configure an IP address and subnet mask if a DHCP server is unavailable at system start time.

5. Why is it important to plan an implementation of DHCP for a network?

   Either WINS or DNS (or possibly both) is used for registering dynamic name-to-address mappings on your network. To provide name resolution services, you must plan for interoperability of DHCP with these services. Most network administrators implementing DHCP also plan a strategy for implementing DNS and WINS servers.

6. What tool do you use to manage DHCP servers in Windows 2000?

   The primary tool that you use to manage DHCP servers is DHCP Manager, which is a Microsoft Management Console (MMC) component that is added to the Administrative Tools menu when you install the DHCP service.

7. What is the symptom of most DHCP-related problems?

   Most DHCP-related problems are identified as a client IP configuration failure. These failures are most often discovered by clients in one of the following ways:

   - **The client might be configured to use an IP address not provided by the server.**
   - **The server sends a negative response back to the client, and the client displays an error message or popup indicating that a DHCP server could not be found.**
   - **The server leases the client an address but the client appears to have other network configuration-based problems, such as the inability to register or resolve DNS or NetBIOS names, or to perceive computers beyond its same subnet.**

Chapter 11

Review Questions

1. What is a VPN?

   A simulated point-to-point connection using encapsulation. This connection can span any underlying network, including the Internet. Security or some form of encryption is usually required to get the "private" part of the definition.

2. Demand-dial filters can screen traffic based on what fields of a packet?

   Source and destination IP address, IP protocol identifier, source and destination ports, ICMP type, and ICMP code.

3. True or false: When setting dial-in user permissions (Allow Access, Deny Access) through the User Property page, RAPs are not used.

   False. In the user interface it appears that RAP is not used. In actuality, the dial-in user settings work in conjunction with RAP.

4. True or False: DHCP packets are never sent over Routing and Remote Access links.

   False. Routing and Remote Access clients do not use DHCP to get an address, but may use DHCPINFORM packets to get other configuration options. The DHCP relay agent must be installed and using the "internal" interface for this to work.

5. What is the function of BAP?

   To bring up or drop modem or ISDN links as needed for bandwidth on demand.

Chapter 12

Review Questions

1. What is the purpose of NAT?

   NAT allows computers on a small network, such as a home office, to share a single Internet connection.

2. What are the components of NAT?

   The translation component is the router on which NAT is enabled. The addressing component provides IP address configuration information to the other computers on the home network. The name resolution component becomes the DNS server for the other computers on the home network. When name resolution requests are received by the NAT computer, it forwards the name resolution requests to the Internet-based DNS server for which it is configured and returns the responses to the home network computer.

3. If a small business is using the 10.0.0.0 private network for its intranet and has been granted the public IP address of 198.200.200.1 by its ISP, to what public IP address does NAT map all private IP addresses being used on network 10.0.0.0?

   The NAT maps (using static or dynamic mappings) all private IP addresses being used on network 10.0.0.0 to the public IP address of 198.200.200.1.

4. What must you do to allow Internet users to access resources on your private network?

   You must configure a static IP address configuration on the resource server including IP address, subnet mask, default gateway, and DNS server. You should exclude the IP address being used by the resource computer from the range of IP addresses being allocated by the NAT computer. Next, you configure a special port, which is a static mapping of a public address and port number to a private address and port number.

Chapter 13

Review Questions

1. What are certificates, and what is their purpose?

   A certificate (digital certificate, public key certificate) is a digital document that attests to the binding of a public key to an entity. The main purpose of a certificate is to generate confidence that the public key contained in the certificate actually belongs to the entity named in the certificate.

2. What is a certificate authority (CA), and what does it do?

   Certificates are issued by a CA, which can be any trusted service or entity willing to vouch for the identities of those to whom it issues certificates, and their association with specific keys.

3. What are the four types of Microsoft certificate authorities?

   Enterprise root CA, enterprise subordinate CA, stand-alone root CA, and stand-alone subordinate CA.

4. Name one reason for a certificate revocation.

   - **Compromise, or suspected compromise, of an entity's private key**
   - **Fraud in obtaining the certificate**
   - **Change in status**

5. What are the five PKI standard certificate stores?

   MY, CA, TRUST, ROOT, and UserDS.

Chapter 14

Review Questions

1. What are some potential security risks you should identify in your security plan?

   It could be possible for competitors to gain access to proprietary product information, or unauthorized users could attempt to maliciously modify Web pages or overload computers so that they are unusable.

2. What is authentication and how can you implement it?

   Authentication is the process of identifying users who attempt to connect to a network. When users are authenticated on your network, they can utilize network resources based on their access permissions. To provide authentication to network users, you establish user accounts.

3. What are some security features of Windows 2000?

   - **Security templates**
   - **Kerberos authentication**
   - **Public key infrastructure (PKI)**
   - **IPSec management**
   - **NT file system encryption**

4. How can you secure a connection between your network and the Internet?

   To secure your organization's network for access to and from the Internet, you can put a firewall between the two networks. The firewall provides connectivity for network users to the Internet while minimizing the risks that connectivity introduces. It also prevents access to computers on your network from the Internet, except for those computers authorized to have such access.

5. What are some remote access protocols you can implement for security?

   Routing and Remote Access can use a secure user authentication method including:

   - **Challenge Handshake Authentication Protocol (CHAP)**
   - **Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)**

- ❖ **Password Authentication Protocol (PAP)**
- ❖ **Shiva Password Authentication Protocol (SPAP)**
- ❖ **Extensible Authentication Protocol (EAP)**

6. Name two forms of encryption available for demand-dial connections.

   Microsoft Point-to-Point Encryption (MPPE) and Internet Protocol Security (IPSec).

7. How do System Monitor and Network Monitor provide the ability to monitor security on your network?

   System Monitor is used to monitor anything from hardware to software, and can also monitor security events such as Errors Access Permissions, Errors Granted Access, Errors Logon, and IIS Security. Network Monitor focuses exclusively on network activity to allow you to understand the traffic and behavior of your network components. If you install the full version available from Systems Management Server, you can capture and view every packet on the network.

8. How is Event Viewer used to monitor security?

   Although you can use Event Viewer to gather information about hardware and software problems, it can also be used to monitor Windows 2000 security events such as valid and invalid logon attempts. The security log can also contain events related to resource use, such as creating, opening, or deleting files or other objects.

9. How do you enable remote access logging in Windows 2000?

   You can enable event logging in the Event Logging tab on the properties of a remote access server in Routing and Remote Access.

Glossary

100VG (Voice Grade) AnyLAN (100VGAnyLAN) An emerging networking technology that combines elements of both Ethernet and Token Ring.

A

access permissions Features that control access to sharing in Windows NT Server. Permissions can be set for the following access levels: No Access—Prevents access to the shared directory, its subdirectories, and its files. Read—Allows viewing of file and subdirectory names, changing to a shared directory's subdirectory, viewing data in files, and running applications. Change—Allows viewing of file and subdirectory names, changing to a shared directory's subdirectories, viewing data in files and running application files, adding files and subdirectories to a shared directory, changing data in files, and deleting subdirectories and files. Full Control—Includes the same permissions as Change, plus changing permissions and taking ownership of files and directories only.

account *See* user account.

account lockout A Windows 2000 security feature that locks a user account if a number of failed logon attempts occur within a specified amount of time, based on security policy lockout settings. Locked accounts cannot log on.

account policy Controls how passwords must be used by all user accounts in a domain or on an individual computer.

Active Directory service The directory service included with Windows 2000 Server. It stores information about objects on a network and makes this information available to users and network administrators. The Active Directory service allows users to use a single logon process to access permitted resources anywhere on the network. The Active Directory service provides network administrators with an intuitive hierarchical view of the network and a single point of administration for all network objects.

Active Directory Service Interfaces (ADSI) A COM-based directory service model that allows ADSI-compliant client applications to access a wide variety of distinct directory protocols, including Windows directory service and Light-weight Directory Access Protocol (LDAP), using a single, standard set of interfaces. ADSI shields the client application from the implementation and operational details of the underlying data store or protocol.

Address Resolution Protocol (ARP) Determines hardware addresses (MAC addresses) that correspond to an Internet Protocol (IP) address.

Administrator A person responsible for setting up and managing domain controllers or local computers and their user and group accounts, assigning passwords and permissions, and helping users with networking issues.

ADSL *See* Asymmetric Digital Subscriber Line (ADSL).

advanced program-to-program communication (APPC) A pecification developed as part of IBM's Systems Network Architecture (SNA) model and designed to enable application programs running on different computers to communicate and exchange data directly. *See also* Systems Network Architecture (SNA).

AFP *See* AppleTalk filing protocol (AFP).

agent A program that performs a background task for a user and reports to the user when the task is done or when some expected event has taken place.

American National Standards Institute (ANSI) An organization of American industry and business groups dedicated to the development of trade and communications standards. ANSI is the American representative to the International Organization for Standardization (ISO). *See also* International Organization for Standardization (ISO).

analog Related to a continuously variable physical property, such as voltage, pressure, or rotation. An analog device can represent an infinite number of values within the range the device can handle. *See also* analog line, digital.

analog line A communications line, such as a telephone line, that carries information in analog (continuously variable) form. To minimize distortion and noise interference, an analog line uses amplifiers to strengthen the signal periodically during transmission.

ANSI *See* American National Standards Institute (ANSI).

APPC *See* advanced program-to-program communication (APPC).

AppleShare AppleShare is the Apple network operating system. Features include file sharing, client software that is included with every copy of the Apple operating system, and the Apple-Share print server, a server-based print spooler.

AppleTalk The Apple network architecture that is included in the Macintosh operating system software. It is a collection of protocols that correspond to the OSI model. Thus, network capabilities are built into every Macintosh. AppleTalk protocols support LocalTalk, Ethernet (EtherTalk), and Token Ring (TokenTalk).

AppleTalk filing protocol (AFP) Describes how files are stored and accessed on the network. AFP is responsible for the Apple hierarchical filing structure of volumes, folders, and files and provides for file sharing between Macintoshes and MS-DOS-based computers. It provides an interface for communication between AppleTalk and other network operating systems, allowing Macintoshes to be integrated into any network that uses an operating system that recognizes AFP.

application programming interface (API) A set of routines that an application program uses to request and carry out lower-level services performed by the operating system.

ArcNet (Attached Resource Computer Network) Developed by Datapoint Corporation in 1977, designed as a baseband, token-passing, bus architecture, transmitting at 2.5 Mbps. A successor to the original ArcNet, ArcNetplus supports data transmission rates of 20 Mbps. A simple, inexpensive, flexible network architecture designed for workgroup-sized LANs, ArcNet runs on coaxial, twisted-pair, and fiber-optic cable and supports up to 255 nodes. ArcNet technology predates IEEE Project 802 standards but loosely maps to the 802.4 document. *See also* IEEE Project 802.

ARP *See* Address Resolution Protocol (ARP).

ARPANET (Advanced Research Projects Agency Network) A pioneering wide area network (WAN) commissioned by the Department of Defense, ARPANET was designed to facilitate the exchange of information between universities and other research organizations. ARPANET, which became operational in the 1960s, is the network from which the Internet evolved.

ASCII (American Standard Code for Information Interchange) A coding scheme that assigns numeric values to letters, numbers, punctuation marks, and certain other characters. By standardizing the values used for these characters, ASCII enables computers and computer programs to exchange information.

Asymmetric Digital Subscriber Line (ADSL) A recent modem technology that converts existing twisted-pair telephone lines into access paths for multimedia and high-speed data communications. These new connections can transmit more than 8

Mbps to the subscriber and up to 1 Mbps from the subscriber. ADSL is recognized as a physical layer transmission protocol for unshielded twisted-pair media.

asynchronous transfer mode (ATM) An advanced implementation of packet switching that provides high-speed data transmission rates to send fixed-size cells over LANs or WANs. Cells are 53 bytes—48 bytes of data with 5 additional bytes of address. ATM accommodates voice, data, fax, real-time video, CD-quality audio, imaging, and multimegabit data transmission. ATM uses switches as multiplexers to permit several computers to put data on a network simultaneously. Most commercial ATM implementations transmit data at about 155 Mbps, but theoretically a rate of 1.2 gigabits per second is possible.

asynchronous transmission A form of data transmission in which information is sent one character at a time, with variable time intervals between characters. Asynchronous transmission does not rely on a shared timer that allows the sending and receiving units to separate characters by specific time periods. Therefore, each transmitted character consists of a number of data bits (that compose the character itself), preceded by a start bit and ending in an optional parity bit followed by a 1-, 1.5-, or 2-stop bit.

ATM *See* asynchronous transfer mode (ATM).

attenuation The weakening or degrading (distorting) of a transmitted signal as it travels farther from its point of origin. This could be a digital signal on a cable or the reduction in amplitude of an electrical signal, without the appreciable modification of the waveform. Attenuation is usually measured in decibels. Attenuation of a signal transmitted over a long cable is corrected by a repeater, which amplifies and cleans up an incoming signal before sending it farther along the cable.

auditing A process that tracks network activities by user accounts and a routine element of network security. Auditing can produce records of list users who have accessed—or attempted to access—specific resources; help administrators identify unauthorized activity; and track activities such as logon attempts, connection and disconnection from designated resources, changes made to files and directories, server events and modifications, password changes, and logon parameter changes.

authentication Verification typically based on user name, password, and time and account restrictions.

authorization A process that verifies that the user has the correct rights or permissions to access a resource.

B

backbone The main cable, also known as the trunk segment, from which transceiver cables connect to computers, repeaters, and bridges.

back end In a client/server application, the part of the program that runs on the server.

backup domain controller (BDC) In a Windows NT Server domain, a computer that receives a copy of the domain's security policy and domain database and authenticates network logons. It provides a backup if the primary domain controller (PDC) becomes unavailable. A domain is not required to have a BDC, but it is recommended to have a BDC to back up the PDC. *See also* domain, domain controller, primary domain controller (PDC).

bandwidth In communications, the difference between the highest and lowest frequencies in a given range. For example, a telephone accommodates a bandwidth of 3000 Hz, or the difference between the lowest (300 Hz) and highest (3300 Hz) frequencies it can carry. In computer networks, greater bandwidth indicates faster or greater data-transfer capability.

baseband A system used to transmit the encoded signals over cable. Baseband uses digital signaling over a single frequency. Signals flow in the form of discrete pulses of electricity or light. With baseband transmission, the entire communication-channel capacity is used to transmit a single data signal.

basic input/output system (BIOS) On PC-compatible computers, the set of essential software routines that test hardware at startup, start the operating system, and support the transfer of data among hardware devices. The BIOS is stored in read-only memory (ROM) so that it can be executed when the computer is turned on. Although critical to performance, the BIOS is usually invisible to computer users.

baud A measure of data-transmission speed named after the French engineer and telegrapher Jean-Maurice-Emile Baudot. It is a measure of the speed of oscillation of the sound wave on which a bit of data is carried over telephone lines. Because baud was originally used to measure the transmission speed of telegraph equipment, the term sometimes refers to the data-transmission speed of a modem. However, current modems can send at a speed higher than 1 bit per oscillation, so baud is being replaced by the more accurate bps (bits per second) as a measure of modem speed.

baud rate Refers to the speed at which a modem can transmit data. Often confused with bps (the number of bits per second transmitted), baud rate actually measures the number of events, or signal changes, that occur in one second.

Because one event can actually encode more than one bit in high-speed digital communication, baud rate and bps are not always synonymous, and the latter is the more accurate term to apply to modems. For example, the 9600-baud modem that encodes 4 bits per event actually operates at 2400 baud, but transmits at 9600 bps (2400 events times 4 bits per event), and thus should be called a 9600-bps modem.

BDC *See* backup domain controller (BDC).

bind To associate two pieces of information with one another.

binding A process that establishes the communication channel between a protocol driver and a NIC driver.

BIOS (basic input/output system) *See* basic input/output system (BIOS).

BISDN *See* Broadband Integrated Services Digital Network (BISDN).

bisync (binary synchronous communications protocol) A communications protocol developed by IBM. Bisync transmissions are encoded in either ASCII or EBCDIC. Messages can be of any length and are sent in units called frames, optionally preceded by a message header. Because bisync uses synchronous transmission, in which message elements are separated by a specific time interval, each frame is preceded and followed by special characters that enable the sending and receiving machines to synchronize their clocks.

bit Short for binary digit: either 1 or 0 in the binary number system. In processing and storage, a bit is the smallest unit of information handled by a computer. It is represented physically by an element such as a single pulse sent through a circuit or small spot on a magnetic disk capable of storing either a 1 or 0. Eight bits make a byte.

bits per second (bps) A measure of the speed at which a device can transfer data. *See also* baud rate.

bit time The time it takes for each station to receive and store a bit.

boot partition The partition that contains the Microsoft Windows 2000 operating system and its support files. The boot partition can be, but does not have to be, the same as the system partition.

bottleneck The limiting factor when analyzing performance of a system or network. Poor performance results when a device uses noticeably more CPU time than it should, consumes too much of a resource, or lacks the capacity to handle the load. Potential bottlenecks can be found in the CPU, memory, NIC, and other components.

bps *See* bits per second (bps).

Broadband Integrated Services Digital Network (BISDN) A consultative committee for the CCITT that recommends definitions for voice, data, and video in the megabit-gigabit range. BISDN is also a single ISDN network that can handle voice, data, and video services. BISDN works with an optical cable transport network called Synchronous Optical Network (SONET) and an asynchronous transfer mode (ATM) switching service. Switched Multimegabit Data Services (SMDS) is a BISDN service that offers high bandwidth to WANs. *See also* Synchronous Optical Network (SONET), asynchronous transfer mode (ATM).

broadband network A type of LAN on which transmissions travel as analog (radio-frequency) signals over separate inbound and outbound channels. Devices on a broadband network are connected by coaxial or fiber-optic cable, and signals flow across the physical medium in the form of electromagnetic or optical waves. A broadband system uses a large portion of the electromagnetic spectrum with a range of frequencies from 50 Mbps to 600 Mbps. These networks can simultaneously accommodate television, voice, data, and other services over multiple transmission channels.

built-in groups One of several group accounts used by Microsoft Windows NT and Windows 2000. Built-in groups, as the name implies, are included with the network operating system. Built-in groups have been granted useful collections of rights and built-in abilities. In most cases, a built-in group provides all the capabilities needed by a particular user. For example, if a domain user account belongs to the built-in Administrators group, logging on with that account gives a user administrative capabilities over the domain and the servers in the domain. *See also* user account.

byte A unit of information consisting of 8 bits. In computer processing or storage, a byte is equivalent to a single character, such as a letter, numeral, or punctuation mark. Because a byte represents only a small amount of information, amounts of computer memory are usually given in kilobytes (1024 bytes or 2 raised to the 10^{th} power), megabytes (1,048,576 bytes or 2 raised to the 20th power), gigabytes (1024 megabytes), terabytes (1024 gigabytes), petabytes (1024 terabytes), or exabytes (1024 petabytes).

C

CA (certificate authority) *See* certificate authority (CA).

carrier-sense multiple access with collision avoidance (CSMA/CA) access method An access method by which each computer signals its intent to transmit before it actually transmits data, thus avoiding possible transmission collisions.

carrier-sense multiple access with collision detection (CSMA/CD) access method An access method generally used with bus topologies. Using CSMA/CD, a station "listens" to the physical medium to determine whether another station is currently transmitting a data frame. If no other station is transmitting, the station sends its data. A station "listens" to the medium by testing the medium for the presence of a carrier, a specific level of voltage or light—thus the term carrier-sense. The multiple access indicates that there are multiple stations attempting to access or put data on the cable at the same time. The collision detection indicates that the stations are also listening for collisions. If two stations attempt to transmit at the same time and a collision occurs, the stations must wait a random period of time before attempting to transmit.

CCEP *See* Commercial COMSEC Endorsement Program (CCEP).

CCITT (Comité Consultatif Internationale de Télégraphie et Téléphonie) An organization based in Geneva, Switzerland, and established as part of the United Nations International Telecommunications Union (ITU). The CCITT recommends use of communication standards that are recognized throughout the world. Protocols established by the CCITT are applied to modems, networks, and facsimile transmission.

Cellular Digital Packet Data (CDPD) A communication standard that uses very fast technology, similar to that of cellular telephones, to offer computer data transmissions over existing analog voice networks between voice calls, when the system is not occupied with voice communication.

certificate A collection of data used for authentication and secure exchange of information on nonsecured networks, such as the Internet. A certificate securely binds a public key to the entity that holds the corresponding private key. Certificates are digitally signed by the issuing CA and can be managed for a user, computer, or service. The most widely accepted format for certificates is defined by ITU-T X.509 international standards.

certificate authority (CA) An entity responsible for establishing the authenticity of public keys belonging to users or other CAs. Activities of a CA may include binding public keys to distinguished names through signed certificates, managing certificate serial numbers, and revoking certificates.

child domain For Domain Name System (DNS), a domain located in the namespace tree directly beneath another directory name (the parent domain). For example, example.Microsoft.com would be a child domain of the Microsoft.com parent domain. A child domain is also called a subdomain.

codec (compression/decompression) Compression/decompression technology for digital video and stereo audio.

Commercial COMSEC Endorsement Program (CCEP) A data-encryption standard introduced by the National Security Agency. Vendors who have the proper security clearance can join CCEP and be authorized to incorporate classified algorithms into communications systems. *See also* encryption.

console Collections of administrative tools.

contention Competition among stations on a network for the opportunity to use a communication line or network resource. Two or more computers attempt to transmit over the same cable at the same time, thus causing a collision on the cable. Such a system needs regulation to eliminate data collisions on the cable that can destroy data and bring network traffic to a halt. *See also* carrier-sense multiple access with collision detection (CSMA/CD) access method.

CRC *See* cyclical redundancy check (CRC).

crosstalk Signal overflow from an adjacent wire. When a second faint telephone conversation is heard in the background while one is making a phone call, crosstalk is occurring.

cryptography The processes, art, and science of keeping messages and data secure. Cryptography is used to enable and ensure confidentiality, data integrity, authentication (entity and data origin), and nonrepudiation.

CSMA/CD *See* carrier-sense multiple access with collision detection (CSMA/CD) access method.

cyclical redundancy check (CRC) A form of error checking in transmitting data. The sending packet includes a number produced by a mathematical calculation made at the transmission source. When the packet arrives at its destination, the calculation is redone. If the two figures are the same, this indicates that the data in the packet has remained stable. If the calculation at the destination differs from the calculation at the source, this indicates that the data has changed during the transmission. In that case, the CRC routine either drops the packet or signals the source computer to retransmit the data.

D

database management system (DBMS) A layer of software between the physical database and the user. The DBMS manages all requests for data-base action from the user, including keeping track of the physical details of file locations and formats, indexing schemes, and so on. In addition, a DBMS permits centralized control of security and data integrity requirements.

Data Communications Equipment (DCE) One of two types of hardware connected by an RS-232 serial connection, the other being a data terminal equipment (DTE) device. A DCE device takes input from a DTE device and often acts as an intermediary device, transforming the input signal in some way before sending it to the actual recipient. For example, an external modem is a DCE device that accepts data from a microcomputer (DTE), modulates it, then sends the data along a telephone connection. In communication, an RS-232 DCE device receives data over line 2 and transmits over line 3. In contrast, a DTE device receives over line 3 and transmits over line 2. *See also* Data Terminal Equipment (DTE).

data encryption *See* encryption.

data encryption standard (DES) A commonly used, highly sophisticated algorithm developed by the U.S. National Bureau of Standards for encrypting and decoding data. *See also* encryption.

data frames Logical, structured packages in which data can be placed. Data being transmitted is segmented into small units and combined with control information such as message start and message end indicators. Each package of information is transmitted as a single unit, called a frame. The data-link layer packages raw bits from the physical layer into data frames. The exact format of the frame used by the network depends on the topology. *See also* frame.

data stream An undifferentiated, byte-by-byte flow of data.

Data Terminal Equipment (DTE) According to the RS-232 hardware standard, a device, such as a microcomputer or a terminal, that has the ability to transmit information in digital form over a cable or a communication line. A DTE is one of two types of hardware connected by an RS-232 serial connection, the other being a DCE (Data Communications Equipment) device, such as a modem, that normally connects the DTE to the communication line itself. In communication, an RS-232 DTE device transmits data over line 2 and receives it over line 3. A DCE receives over line 2 and transmits over line 3. *See also* Data Communications Equipment (DCE).

DBMS *See* database management system (DBMS).

DCE *See* Data Communications Equipment (DCE).

DECnet Digital Equipment Corporation hardware and software products that implement the Digital Network Architecture (DNA). DECnet defines communication networks over Ethernet LANs, Fiber Distributed Data Interface metropolitan area networks (FDDI MANs), and WANs that use private or public data transmission facilities. It can use TCP/IP and OSI protocols as well as Digital's DECnet protocols.

See also Fiber Distributed Data Interface (FDDI), metropolitan area network (MAN).

dedicated server A computer on a network that functions only as a server and is not also used as a client.

DES *See* data encryption standard (DES).

Dfs (Distributed File System) *See* Distributed File System (Dfs).

DHCP *See* Dynamic Host Configuration Protocol (DHCP).

DHCP client Any network-enabled device that supports the ability to communicate with a DHCP server for the purpose of obtaining dynamic leased Internet Protocol (IP) configuration and related optional parameters information.

DHCP scope A range of Internet Protocol (IP) addresses that are available to be leased or assigned to DHCP clients by the DHCP service.

DHCP server In Microsoft Windows 2000 Server, a computer running the Microsoft DHCP service that offers dynamic configuration of Internet Protocol (IP) addresses and related information to DHCP-enabled clients.

dial-up connection The connection to your network if you are using a device that uses the telephone network. This includes modems with a standard phone line, ISDN cards with high-speed ISDN lines, or X.25 networks. If you are a typical user, you may have one or two dial-up connections, perhaps to the Internet and to your corporate network. In a more complex server situation, multiple network modem connections might be used to implement advanced routing.

digital A system that encodes information numerically, such as 0 and 1, in a binary context. Computers use digital encoding to process data. A digital signal is a discrete binary state, either on or off. *See also* analog.

digital line A communication line that carries information only in binary-encoded (digital) form. To minimize distortion and noise interference, a digital line uses repeaters to regenerate the signal periodically during transmission. *See also* analog line.

digital signature A means for originators of a message, file, or other digitally encoded information to bind their identity to the information. The process of signing information entails transforming the information, as well as some secret information held by the sender, into a tag called a signature. Digital signatures are used in public key environments and they provide nonrepudiation and integrity services.

directory service Provides the methods for storing directory data and making this data available to network users and administrators. For example, Active Directory stores information about user accounts, such as names, passwords, phone numbers, and so on, and enables other authorized users on the same network to access this information.

Distributed File System (Dfs) A single, logical, hierarchical file system. Dfs organizes shared folders on different computers in a network to provide a logical tree structure for file system resources.

DNS *See* Domain Name System (DNS).

domain For Microsoft networking, a collection of computers and users that share a common database and security policy that are stored on a Windows NT Server domain controller. Each domain has a unique name. *See also* workgroup.

domain controller For Microsoft networking, the Windows NT Server-based computer that authenticates domain logons and maintains the security policy and master database for a domain. *See also* backup domain controller (BDC), primary domain controller (PDC).

domain model A grouping of one or more domains with administration and communication links between them that is arranged for the purpose of user and resource management.

domain namespace The database structure used by the Domain Name System (DNS).

Domain Name System (DNS) A general-purpose distributed, replicated, data-query service used primarily on the Internet for translating host names into Internet addresses.

downtime The amount of time a computer system or associated hardware remains nonfunctioning. Although downtime can occur because hardware fails unexpectedly, it can also be a scheduled event, such as when a network is shut down to allow time for maintaining the system, changing hardware, or archiving files.

driver A software component that permits a computer system to communicate with a device. For example, a printer driver is a device driver that translates computer data into a form understood by the target printer. In most cases, the driver also manipulates the hardware to transmit the data to the device.

DTE *See* Data Terminal Equipment (DTE).

duplex transmission Also called full-duplex transmission. Communication that takes place simultaneously, in both directions, between the sender and the receiver. Alternative methods of transmission are simplex, which is one way only, and half-duplex, which is two-way communication that occurs in only one direction at a time.

Dynamic Host Configuration Protocol (DHCP) A protocol for automatic TCP/IP configuration that provides static and dynamic address allocation and management. *See also* Transmission Control Protocol/Internet Protocol (TCP/IP).

E

EBCDIC *See* Extended Binary Coded Decimal Interchange Code (EBCDIC).

EFS (encrypting file system) *See* encrypting file system (EFS).

encrypting file system (EFS) Windows 2000 file system that enables users to encrypt files and folders on an NTFS volume to keep them safe from intruders who have physical access to the disk.

encryption The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission or when the data is stored on a transportable magnetic medium. A key is required to decode the information. *See also* Commercial COMSEC Endorsement Program (CCEP), data encryption standard (DES).

Ethernet A LAN developed by Xerox in 1976. Ethernet became a widely implemented network from which the IEEE 802.3 standard for contention networks was developed. It uses a bus topology, and the original Ethernet relies on CSMA/CD to regulate traffic on the main communication line.

EtherTalk Allows the AppleTalk network protocols to run on Ethernet coaxial cable. The EtherTalk card allows a Macintosh computer to connect to an 802.3 Ethernet network. *See also* AppleTalk.

event An action or occurrence to which a program might respond. Examples of events are mouse clicks, key presses, and mouse movements. Also, any significant occurrence in the system or in a program that requires users to be notified or an entry to be added to a log.

Extended Binary Coded Decimal Interchange Code (EBCDIC) A coding scheme developed by IBM for use with IBM mainframe and personal computers as a standard method of assigning binary (numeric) values to alphabetic, numeric, punctuation, and transmission-control characters.

extended partition A portion of a basic disk that can contain logical drives. Use an extended partition if you want to have more than four volumes on your basic disk. Only one of the four partitions allowed per physical disk can be an extended partition, and no primary partition needs to be present to create an extended partition. Extended partitions can be created only on basic disks.

F

FAT (file allocation table) *See* file allocation table (FAT).

fault tolerance The ability of a computer or an operating system to respond to an event such as a power outage or a hardware failure in such a way that no data is lost and any work in progress is not corrupted.

Fiber Distributed Data Interface (FDDI) A standard developed by the ANSI for high-speed, fiber-optic local area networks. FDDI provides specifications for transmission rates of 100 Mbps on networks based on the Token Ring standard.

fiber-optic cable Cable that uses optical fibers to carry digital data signals in the form of modulated pulses of light.

file allocation table (FAT) A table or list maintained by some operating systems to keep track of the status of various segments of disk space used for file storage.

file replication service (FRS) Provides multimaster file replication for designated directory trees between Windows 2000 servers. The directory trees must be on disk partitions formatted with the version of NTFS used with Windows 2000. FRS is used by the Microsoft Distributed File System (Dfs) to automatically synchronize content between assigned replicas, and by Active Directory to automatically synchronize content of the system volume information across domain controllers.

File Transfer Protocol (FTP) A process that provides file transfers between local and remote computers. FTP supports several commands that allow bidirectional transfer of binary and ASCII files between computers. The FTP client is installed with the TCP/IP connectivity utilities. *See also* ASCII (American Standard Code for Information Interchange), Transmission Control Protocol/Internet Protocol (TCP/IP).

firewall A security system, usually a combination of hardware and software, intended to protect a network against external threats coming from another network, including the Internet. Firewalls prevent an organization's networked computers from communicating directly with computers that are external to the network, and vice versa. Instead, all incoming and outgoing communication is routed through a proxy server outside the organization's network. Firewalls also

audit network activity, recording the volume of traffic and information about unauthorized attempts to gain access. *See also* proxy server.

FQDN (fully qualified domain name) *See* fully qualified domain name (FQDN).

frame A package of information transmitted on a network as a single unit. Frame is a term most often used with Ethernet networks. A frame is similar to the packet used in other networks. *See also* data frames, packet.

frame preamble Header information, added to the beginning of a data frame in the physical layer of the OSI reference model.

frame relay An advanced, fast-packet, variable-length, digital, packet-switching technology. It is a point-to-point system that uses a private virtual circuit (PVC) to transmit variable-length frames at the data-link layer of the OSI reference model. Frame relay networks can also provide subscribers with bandwidth, as needed, that allows users to make nearly any type of transmission.

front end In a client/server application, front end refers to the part of the program carried out on the client computer.

FRS (file replication service) *See* file replication service (FRS).

FTP *See* File Transfer Protocol (FTP).

full-duplex transmission Also called duplex transmission. Communication that takes place simultaneously in both directions. *See also* duplex transmission.

fully qualified domain name (FQDN) A DNS domain name that has been stated unambiguously so as to indicate with absolute certainty its location in the domain namespace tree. Fully qualified domain names differ from relative names in that they can be stated with a trailing period (.), for example, host.example.microsoft.com, to qualify their position to the root of the namespace.

G

global group One of four kinds of group accounts used by Microsoft Windows NT and Windows NT Server. Used across an entire domain, global groups are created on a primary domain controller (PDC) in the domain in which the user accounts reside. Global groups can contain only user accounts from the domain in which the global group is created. Members of global groups obtain resource permissions when the global group is added to a local group. *See also* group, primary domain controller (PDC).

group In networking, an account containing other accounts that are called members. The permissions and rights granted to a group are also provided to its members; thus, groups offer a convenient way to grant common capabilities to collections of user accounts.

H

half-duplex transmission Two-way communication occurring in only one direction at a time.

handshaking A term applied to modem-to-modem communication. Refers to the process by which information is transmitted between the sending and receiving devices to maintain and coordinate data flow between them. Proper handshaking ensures that the receiving device will be ready to accept data before the sending device transmits.

HDLC *See* High-Level Data Link Control (HDLC).

header In network data transmission, one of the three sections of a packet component. It includes an alert signal to indicate that the packet is being transmitted, the source address, the destination address, and clock information to synchronize transmission.

hierarchical namespace A namespace, such as the Domain Name System (DNS) and Active Directory, that has a tiered structure allowing names and objects to be nested within each other.

High-Level Data Link Control (HDLC) HDLC is a widely accepted international protocol, developed by the International Organization for Standardization (ISO), that governs information transfer. HDLC is a bit-oriented, synchronous protocol that applies to the data-link (message packaging) layer of the OSI reference model. Under the HDLC protocol, data is transmitted in frames, each of which can contain a variable amount of data, but must be organized in a particular way. *See also* data frames, frame.

hop In routing through a mesh environment, the transmission of a data packet through a router.

host name The name of a device on a network. For a device on a Windows 2000 network, this can be the same as the computer name.

HTML *See* Hypertext Markup Language (HTML).

Hypertext Markup Language (HTML) A language developed for writing pages for the World Wide Web. HTML allows text to include codes that define fonts, layout, embedded graphics, and hypertext links. Hypertext provides a method for presenting text, images, sound, and videos that are linked together in a nonsequential web of associations.

Hypertext Transfer Protocol (HTTP) The method by which World Wide Web pages are transferred over the network.

I

IAB *See* Internet Architecture Board (IAB).

IBM cabling system Used in a Token Ring environment. Introduced by IBM in 1984 to define cable connectors, face plates, distribution panels, and cable types. Many parameters are similar to non-IBM specifications. Uniquely shaped, the IBM connector is hermaphroditic.

ICMP *See* Internet Control Message Protocol (ICMP).

IEEE *See* Institute of Electrical and Electronics Engineers (IEEE).

IEEE Project 802 A networking model developed by the IEEE. Named for the year and month it began (February 1980), Project 802 defines LAN standards for the physical and data-link layers of the OSI reference model. Project 802 divides the data-link layer into two sublayers: Media Access Control (MAC) and Logical Link Control (LLC).

incremental backup Backs up only the files created or changed since the last normal (or incremental) backup, and marks the files as having been backed up.

infrared transmission Electromagnetic radiation with frequencies in the electromagnetic spectrum in the range just below that of visible red light. In network communications, infrared technology offers extremely high transmission rates and wide bandwidth in line-of-sight communications.

Institute of Electrical and Electronics Engineers (IEEE) An organization of engineering and electronics professionals; noted in networking for developing the IEEE 802.x standards for the physical and data-link layers of the OSI reference model, applied in a variety of network configurations.

Integrated Services Digital Network (ISDN) A worldwide digital communication network that evolved from existing telephone services. The goal of the ISDN is to replace current telephone lines, which require digital-to-analog conversions, with completely digital switching and transmission facilities capable of carrying data ranging from voice to computer transmissions, music, and video. The

ISDN is built on two main types of communications channels: B channels that carry voice, data, or images at a rate of 64 Kbps, and a D channel that carries control information, signaling, and link-management data at 16 Kbps. Standard ISDN Basic Rate desktop service is called 2B+D. Computers and other devices connect to ISDN lines through simple, standardized interfaces.

International Organization for Standardization (ISO) An organization made up of standards-setting groups from various countries. For example, the United States member is the American National Standards Institute (ANSI). The ISO works to establish global standards for communications and information exchange. Primary among its accomplishments is development of the widely accepted OSI reference model. Note that the ISO is often wrongly identified as the International Standards Organization, probably because of the abbreviation ISO; however, ISO is derived from *isos,* which means equal in Greek, rather than an acronym.

International Telecommunications Union (ITU) The organization responsible for setting the standards for international telecommunications.

International Telecommunications Union-Telecom-munication (ITU-T) The sector of the ITU responsible for telecommunication standards. Its responsibilities include standardizing modem design and operations and standardizing protocols for networks and facsimile transmission. ITU is an international organization within which governments and the private sector coordinate global telecom networks and services.

Internet Architecture Board (IAB) A body that develops and maintains Internet architectural standards as part of the Internet Society (ISOC). It also adjudicates disputes in the standards process.

Internet Control Message Protocol (ICMP) Used by IP and higher-level protocols to send and receive status reports about information being transmitted.

Internet Information Services (IIS) Software services that support Web site creation, configuration, and management, along with other Internet functions. Microsoft Internet Information Services include Network News Transfer Protocol (NNTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP).

Internet Protocol (IP) The TCP/IP protocol for packet forwarding. *See also* Transmission Control Protocol/Internet Protocol (TCP/IP).

internetworking The intercommunication in a network that is made up of smaller networks.

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) A protocol stack that is used in Novell networks. IPX is the NetWare protocol for packet forwarding and routing. It is a relatively small and fast protocol on a LAN, is

a derivative of Xerox Network System (XNS), and supports routing. SPX is a connection-oriented protocol used to guarantee the delivery of the data being sent. NWLink is the Microsoft implementation of the IPX/SPX protocol.

IP *See* Internet Protocol (IP). *See also* Transmission Control Protocol/Internet Protocol (TCP/IP).

IP address A 32-bit address used to identify a node on an IP network. Each node on the IP network must be unique. An IP address consists of a network identifier and a host identifier. This address is typically represented in dotted-decimal notation, with the decimal value of each octet separated by a period, for example, 192.168.7.27. In Microsoft Windows 2000, you can configure the IP address statically or dynamically through DHCP.

ipconfig A diagnostic command that displays all current TCP/IP network configuration values. It is of particular use on systems running DHCP because it allows users to determine which TCP/IP configuration values have been configured by the DHCP server. *See also* winipcfg.

IPX/SPX *See* Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX).

ISDN *See* Integrated Services Digital Network (ISDN).

ISO *See* International Organization for Standardization (ISO).

ITU *See* International Telecommunications Union (ITU).

ITU-T *See* International Telecommunications Union-Telecommunication (ITU-T).

K

Kerberos V5 An Internet standard security protocol for handling authentication of user or system identity. With Kerberos V5, passwords that are sent across network lines are encrypted, not sent as plaintext. Kerberos V5 also includes other security features.

L

LAN *See* local area network (LAN).

LAN requester *See* requester (LAN requester).

LAT *See* local area transport (LAT).

Layer 2 Tunneling Protocol (L2TP) An industry standard Internet tunneling protocol. Unlike Point-to-Point Tunneling Protocol (PPTP), L2TP does not require Internet Protocol (IP) connectivity between the client workstation and the server.

L2TP requires only that the tunnel medium provide packet-oriented point-to-point connectivity. The protocol can be used over media such as Asynchronous Transfer Mode (ATM), frame relay, and X.25. L2TP provides the same functionality as PPTP. Based on Layer 2 Forwarding (L2F) and PPTP specifications, L2TP allows clients to set up tunnels across intervening networks.

layering The coordination of various protocols in a specific architecture that allows the protocols to work together to ensure that the data is prepared, transferred, received, and acted on as intended.

load balancing A technique used to scale the performance of a server-based program (such as a Web server) by distributing its client requests across multiple servers within the cluster. Typically, each host can specify the load percentage that it will handle, or the load can be equally distributed across all the hosts. If a host fails, the load is dynamically redistributed among the remaining hosts.

local area network (LAN) Computers connected in a geographically confined network, such as in the same building, campus, or office park.

local area transport (LAT) A nonroutable protocol from Digital Equipment Corporation.

local group One of four kinds of group accounts used by Microsoft Windows NT and Windows NT Server. Implemented in each local computer's account database, local groups contain user accounts and other global groups that need to have access, rights, and permissions assigned to a resource on a local computer. Local groups cannot contain other local groups.

LocalTalk Cabling components used in an AppleTalk network, including cables, connector modules, and cable extenders. These components are normally used in a bus or tree topology. A LocalTalk segment supports a maximum of 32 devices. Because of LocalTalk's limitations, clients often turn to vendors other than Apple for AppleTalk cabling. Farallon PhoneNet, for example, can accommodate 254 devices.

M

MAN (metropolitan area network) *See* metropolitan area network (MAN).

media The vast majority of LANs today are connected by some sort of wire or cabling that acts as the LAN transmission medium, carrying data between computers. The cabling is often referred to as the media.

metropolitan area network (MAN) A data network designed for a town or city. In geographic breadth, MANs are larger than local area networks but smaller than

wide area networks. MANs are usually characterized by very-high-speed connections using fiber-optic cable or other digital media.

Microsoft Management Console (MMC) A framework for hosting administrative tools, called consoles. A console may contain tools, folders, or other containers, World Wide Web pages, and other administrative items. These items are displayed in the left pane of the console, called a console tree. A console has one or more windows that can provide views of the console tree. The main MMC window provides commands and tools for authoring consoles. The authoring features of MMC and the console tree itself may be hidden when a console is in User Mode.

Microsoft Technical Information Network (TechNet) Provides informational support for all aspects of networking, with an emphasis on Microsoft products.

mixed mode The default domain mode setting on Microsoft Windows 2000 domain controllers. Mixed mode allows Windows NT and Windows 2000 backup domain controllers to coexist in a domain. Mixed mode does not support the universal and nested group enhancements of Windows 2000. The domain mode setting can be changed to Windows 2000 native mode when all Windows NT domain controllers are removed from a domain.

MMC (Microsoft Management Console) *See* Microsoft Management Console (MMC).

N

name resolution The process of translating a name into some object or information that the name represents. A telephone book forms a namespace in which the names of the telephone subscribers can be resolved to telephone numbers. The Microsoft Windows NT file system (NTFS) forms a namespace in which the name of a file can be resolved to the file itself. The Active Directory forms a namespace in which the name of an object in the directory can be resolved to the object itself.

namespace A set of unique names for resources or items used in a shared computing environment. For MMC, the namespace is represented by the console tree, which displays all of the snap-ins and resources that are accessible to a console. *See also* Microsoft Management Console (MMC), resource, snap-in. For DNS, namespace is the vertical or hierarchical structure of the domain name tree. For example, each domain label, such as host1 or example, used in a fully qualified domain name, such as host1.example. microsoft.com, indicates a branch in the domain namespace tree.

NAS (network access server) *See* network access server (NAS).

nbtstat A diagnostic command that displays protocol statistics and current TCP/IP connections using NBT (NetBIOS over TCP/IP). This command is available only if the TCP/IP protocol has been installed. *See also* netstat.

NDIS *See* Network Device Interface Specification (NDIS).

NetBEUI (NetBIOS Enhanced User Interface) A protocol supplied with all Microsoft network products. NetBEUI advantages include small stack size (important for MS-DOS-based computers), speed of data transfer on the network medium, and compatibility with all Microsoft-based networks. The major drawback of NetBEUI is that it is a LAN transport protocol and therefore does not support routing. It is also limited to Microsoft-based networks.

NetBIOS (network basic input/output system) An application programming interface (API) that can be used by application programs on a LAN consisting of IBM-compatible microcomputers running MS-DOS, OS/2, or some version of UNIX. Primarily of interest to programmers, NetBIOS provides application programs with a uniform set of commands for requesting the lower-level network services required to conduct sessions between nodes on a network and transmit

information between them.

netstat A diagnostic command that displays protocol statistics and current TCP/IP network connections. This command is available only if the TCP/ IP protocol has been installed. *See also* nbtstat.

network access server (NAS) The device that accepts PPP connections and places clients on the network that the NAS serves.

Network Device Interface Specification (NDIS) A standard that defines an interface for communication between the Media Access Control (MAC) sublayer and protocol drivers. NDIS allows for a flexible environment of data exchange. It defines the software interface, called the NDIS interface, which is used by protocol drivers to communicate with the network interface card. The advantage of NDIS is that it offers protocol multiplexing so that multiple protocol stacks can be used at the same time.

network monitors Monitors that track all or a selected part of network traffic. They examine frame-level packets and gather information about packet types, errors, and packet traffic to and from each computer.

Network News Transfer Protocol (NNTP) A protocol defined in RFC 977. It is a de facto protocol standard on the Internet used for the distribution, inquiry, retrieval, and posting of Usenet news articles over the Internet.

NNTP *See* Network News Transfer Protocol (NNTP).

Novell NetWare One of the leading network architectures.

NSLOOKUP A command-line utility that allows you to make Domain Name System (DNS) queries for testing and troubleshooting your DNS installation.

NTFS *See* NTFS file system.

NTFS file system An advanced file system designed for use specifically within the Microsoft Windows 2000 operating system. It supports file system recovery, extremely large storage media, long filenames, and various features for the Portable Operating System Interface for UNIX (POSIX) subsystem. It also supports object-oriented applications by treating all files as objects with user-defined and system-defined attributes.

O

object An entity such as a file, folder, shared folder, printer, or Active Directory object described by a distinct, named set of attributes. For example, the attributes of a file object include its name, location, and size; the attributes of an Active Directory user object might include the user's first name, last name, and e-mail address.

Open Shortest Path First (OSPF) A routing protocol for IP networks, such as the Internet, that allows a router to calculate the shortest path to each node for sending messages.

Open Systems Interconnection (OSI) reference model A seven-layer architecture that standardizes levels of service and types of interaction for computers exchanging information through a network. It is used to describe the flow of data between the physical connection to the network and the end-user application. This model is the best known and most widely used model for describing networking environments.

OSI *See* Open Systems Interconnection (OSI) reference model.

OSPF *See* Open Shortest Path First (OSPF).

P

packet A unit of information transmitted as a whole from one device to another on a network. In packet-switching networks, a packet is defined more specifically as a transmission unit of fixed maximum size that consists of binary digits representing data; a header containing an identification number, source, and destination addresses; and sometimes error-control data. *See also* frame.

Packet Internet Groper (ping) A simple utility that tests if a network connection is complete, from the server to the workstation, by sending a message to the

remote computer. If the remote computer receives the message, it responds with a reply message. The reply consists of the remote workstation's IP address, the number of bytes in the message, how long it took to reply—given in milliseconds (ms)—and the length of Time to Live (TTL) in seconds. Ping works at the IP level and will often respond even when higher-level TCP-based services cannot.

packet switching A message delivery technique in which small units of information (packets) are relayed through stations in a computer network along the best route available between the source and the destination. Data is broken into smaller units and then repacked in a process called packet assembly and disassembly (PAD). Although each packet can travel along a different path, and the packets composing a message can arrive at different times or out of sequence, the receiving computer reassembles the original message. Packet-switching networks are considered fast and efficient. Standards for packet switching on networks are documented in the CCITT recommendation X.25.

page-description language (PDL) A language that communicates to a printer how printed output should appear. The printer uses the PDL to construct text, and graphics to create the page image. PDLs are like blueprints in that they set parameters and features such as type sizes and fonts, but leave the drawing to the printer.

PBX Private Branch Exchange (PABX Private Automated Branch Exchange) A switching telephone network that allows callers within an organization to place intraorganizational calls without going through the public telephone system.

PDC *See* primary domain controller (PDC).

PDL *See* page-description language (PDL).

PDN *See* public data network (PDN).

performance counter In System Monitor, a data item associated with a performance object. For each counter selected, System Monitor presents a value corresponding to a particular aspect of the performance defined for the performance object.

performance monitor A tool for monitoring network performance that can display statistics, such as the number of packets sent and received, server-processor utilization, and the amount of data going into and out of the server.

performance object In System Monitor, a logical collection of counters that is associated with a resource or service that can be monitored.

ping *See* Packet Internet Groper (ping).

PKI (public key infrastructure) *See* public key infrastructure (PKI).

pointer (PTR) resource record A resource record used in a reverse lookup zone created within the in-addr.arpa domain to designate a reverse mapping of a host Internet Protocol (IP) address to a host Domain Name System (DNS) domain name.

point-to-point configuration Dedicated circuits that are also known as private, or leased, lines. They are the most popular WAN communication circuits in use today. The carrier guarantees full-duplex bandwidth by setting up a permanent link from each endpoint, using bridges and routers to connect LANs through the circuits. *See also* Point-to-Point Protocol (PPP), Point-to-Point Tunneling Protocol (PPTP), duplex transmission.

Point-to-Point Protocol (PPP) A data-link protocol for transmitting TCP/IP packets over dial-up telephone connections, such as between a computer and the Internet. PPP was developed by the Internet Engineering Task Force in 1991.

Point-to-Point Tunneling Protocol (PPTP) PPTP is an extension of the Point-to-Point Protocol that is used for communication on the Internet. It was developed by Microsoft to support virtual private networks (VPNs), which allow individuals and organizations to use the Internet as a secure means of communication. PPTP supports encapsulation of encrypted packets in secure wrappers that can be transmitted over a TCP/IP connection. *See also* virtual private network (VPN).

PPP *See* Point-to-Point Protocol (PPP).

PPTP *See* Point-to-Point Tunneling Protocol (PPTP).

primary domain controller (PDC) The server that maintains the master copy of the domain's user-accounts database and validates logon requests. Every network domain is required to have one, and only one, PDC. *See also* domain, domain controller.

primary zone database file The master zone database file. Changes to a zone, such as adding domains or hosts, are performed on the server that contains the primary zone database file.

private key The secret half of a cryptographic key pair that is used with a public key algorithm. Private keys are typically used to decrypt a symmetric session key, digitally sign data, or decrypt data that has been encrypted with the corresponding public key.

protocol The system of rules and procedures that govern communication between two or more devices. Many varieties of protocols exist, and not all are compatible,

but as long as two devices are using the same protocol, they can exchange data. Protocols exist within protocols as well, governing different aspects of communication. Some protocols, such as the RS-232 standard, affect hardware connections. Other standards govern data transmission, including the parameters and handshaking signals such as XON/OFF used in asynchronous (typically, modem) communications, as well as such data-coding methods as bit- and byte-oriented protocols. Still other protocols, such as the widely used XMODEM, govern file transfer, and others, such as CSMA/ CD, define the methods by which messages are passed around the stations on a LAN. Protocols represent attempts to ease the complex process of enabling computers of different makes and models to communicate. Additional examples of protocols include the OSI model, IBM's SNA, and the Internet suite, including TCP/IP. *See also* Systems Network Architecture (SNA), Transmission Control Protocol/Internet Protocol (TCP/IP).

protocol driver The driver responsible for offering four or five basic services to other layers in the network, while "hiding" the details of how the services are actually implemented. Services performed include session management, datagram service, data segmentation and sequencing, acknowledgment, and possibly routing across a WAN.

protocol stack A layered set of protocols that work together to provide a set of network functions.

proxy server A firewall component that manages Internet traffic to and from a local area network (LAN). The proxy server decides whether it is safe to let a particular message or file pass through to the organization's network, providing access control to the network, and filters and discards requests as specified by the owner, including requests for unauthorized access to proprietary data. *See also* firewall.

public data network (PDN) A commercial packet-switching or circuit-switching WAN service provided by local and long-distance telephone carriers.

public key The nonsecret half of a cryptographic key pair that is used with a public key algorithm. Public keys are typically used when encrypting a session key, verifying a digital signature, or encrypting data that can be decrypted with the corresponding private key.

public key cryptography A method of cryptography in which two different keys are used: a public key for encrypting data and a private key for decrypting data.

public key infrastructure (PKI) The term generally used to describe the laws, policies, standards, and software that regulate or manipulate certificates and public and private keys. In practice, it is a system of digital certificates, certification authorities, and other registration authorities that verify and authenticate the validity of each party involved in an electronic transaction. Standards for PKI are still evolving, even though they are being widely implemented as a necessary element of electronic commerce.

Q

QoS (quality of service) *See* quality of service (QoS).

quality of service (QoS) A set of quality-assurance standards and mechanisms for data transmission, implemented in Windows 2000.

R

RADIUS (Remote Authentication Dial-In User Service) *See* Remote Authentication Dial-In User Service (RADIUS).

RAS *See* Remote Access Server (RAS).

redirector Networking software that accepts I/O requests for remote files, named pipes, or mail slots, and sends (redirects) the requests to a

network service on another computer.

Remote Access Server (RAS) Any Microsoft Windows 2000-based computer configured to accept remote access connections.

Remote Authentication Dial-In User Service (RADIUS) A security authentication protocol based on clients and servers and widely used by Internet service providers (ISPs) on non-Microsoft remote servers. RADIUS is the most popular means of authenticating and authorizing dial-up and tunneled network users today.

remote computer A computer that can be accessed only by using a communications line or a communications device, such as a network card or a modem.

remote user A user who dials in to the server over modems and telephone lines from a remote location.

Request for Comments (RFC) The official documents of the Internet Engineering Task Force (IETF) that specify the details for protocols included in the Transmission Control Protocol/Internet Protocol (TCP/IP) family.

requester (LAN requester) Software that resides in a computer and forwards requests for network services from the computer's application programs to the appropriate server. *See also* redirector.

resource Any part of a computer system. Users on a network can share computer resources, such as hard disks, printers, modems, CD-ROM drives, and even the processor.

resource record Standard database record types used in zones to associate Domain Name System (DNS) domain names to related data for a given type of network resource, such as a host Internet Protocol (IP) address. Most of the basic resource record types are defined in RFC 1035, but additional resource record types are defined in other RFCs and approved for use with DNS.

reverse lookup In Domain Name System (DNS), a query process by which the Internet Protocol (IP) address of a host computer is searched to find its friendly DNS domain name.

RFC *See* Request for Comments (RFC).

RIP *See* Routing Information Protocol (RIP).

Routing Information Protocol (RIP) A protocol that uses distance-vector algorithms to determine routes. With RIP, routers transfer information among other routers to update their internal routing tables, and use that information to determine the best routes based on hop counts between routers. TCP/IP and IPX support RIP.

S

SAP (service access point) *See* service access point (SAP).

SAP (Service Advertising Protocol) *See* Service Advertising Protocol (SAP).

SDLC *See* Synchronous Data Link Control (SDLC).

secondary master An authoritative Domain Name System (DNS) server for a zone that is used as a source for replication of the zone to other servers. Secondary masters update their zone data only by transferring zone data from other DNS servers. They do not have the ability to perform zone updates.

security Making computers and data stored on them safe from harm or unauthorized access.

security identifier or **security ID (SID)** A unique number that identifies user, group, and computer accounts. Every account on your network is issued a unique SID when the account is first created. Internal processes in Windows 2000 refer to an account's SID rather than the account's user or group name. If you create an

account, delete it, and then create an account with the same user name, the new account will not have the rights or permissions previously granted to the old account because the accounts have different SID numbers.

segment The length of cable on a network between two terminators. A segment can also refer to messages that have been broken up into smaller units by the protocol driver.

Sequenced Packet Exchange (SPX) Part of Novell's IPX/SPX protocol suite for sequenced data. *See also* Internetwork Packet Exchange/ Sequenced Packet Exchange (IPX/SPX).

Serial Line Internet Protocol (SLIP) Defined in RFC 1055. SLIP is normally used on Ethernet, over a serial line; for example, an RS-232 serial port connected to a modem.

serial transmission One-way data transfer. The data travels on a network cable with one bit following another.

server message block (SMB) The protocol developed by Microsoft, Intel, and IBM that defines a series of commands used to pass information between network computers. The redirector packages SMB requests into a network control block (NCB) structure that can be sent over the network to a remote device. The network provider listens for SMB messages destined for it and removes the data portion of the SMB request so that it can be processed by a local device.

service A program, routine, or process that performs a specific system function to support other programs, particularly at the hardware level. When services are provided over a network, they can be published in Active Directory, facilitating service-centric administration and usage. Some examples of Microsoft Windows 2000 services are Security Accounts Manager service, File Replication service, and Routing and Remote Access service.

service access point (SAP) The interface among each of the seven layers in the OSI protocol stack that has connection points, similar to addresses, used for communication among layers. Any protocol layer can have multiple SAPs active at one time.

Service Advertising Protocol (SAP) Allows service-providing nodes (including file, printer, gateway, and application servers) to advertise their services and addresses.

service (SRV) resource record A resource record used in a zone to register and locate well-known Transmission Control Protocol/Internet Protocol (TCP/IP) services. The SRV resource record is specified in RFC 2052 and is used in Microsoft Windows 2000 or later to locate domain controllers for Active Directory service.

session management Establishing, maintaining, and terminating connections between stations on the network.

shell A piece of software, usually a separate program, that provides direct communication between the user and the operating system. This usually, but not always, takes the form of a command-line interface. Examples of shells are Macintosh Finder and the MS-DOS command interface program COMMAND.COM.

SID (security identifier or **security ID)** *See* security identifier or security ID (SID).

Simple Mail Transfer Protocol (SMTP) A TCP/IP protocol for transferring e-mail. *See also* Transmission Control Protocol/Internet Protocol (TCP/IP).

Simple Network Management Protocol (SNMP) A TCP/IP protocol for monitoring networks. SNMP uses a request and response process. In SNMP, short utility programs, called agents, monitor the network traffic and behavior in key network components to gather statistical data, which they put into a management information base (MIB). To collect the information into a usable form, a special management console program regularly polls the agents and downloads the information in their MIBs. If any of the data falls either above or below parameters set by the manager, the management console program can present signals on the monitor locating the trouble and notify designated support staff by automatically dialing a pager number.

SLIP *See* Serial Line Internet Protocol (SLIP).

smart card A credit card-sized device used to securely store public and private keys, passwords, and other types of personal information. To use a smart card, you need a smart card reader attached to the computer and a personal identification number for the smart card. In Windows 2000, smart cards can be used to enable certificate-based authentication and single sign-on to the enterprise.

smart card reader A standard device within the smart card subsystem. A smart card reader is an interface device (IFD) that supports bidirectional input/output to a smart card.

SMB *See* server message block (SMB).

SMTP *See* Simple Mail Transfer Protocol (SMTP).

SNA *See* Systems Network Architecture (SNA).

snap-in A type of tool you can add to a console supported by Microsoft Management Console (MMC). A stand-alone snap-in can be added by itself; an extension snap-in can only be added to extend the function of another snap-in.

SNMP *See* Simple Network Management Protocol (SNMP).

SONET *See* Synchronous Optical Network (SONET).

SPX *See* Sequenced Packet Exchange (SPX).

SQL *See* structured query language (SQL).

stand-alone computer A computer that is not connected to any other computers and is not part of a network.

stand-alone server A computer that runs Microsoft Windows 2000 Server but does not participate in a domain. A stand-alone server has only its own database of users, and it processes logon requests by itself. It does not share account information with any other computer and cannot provide access to domain accounts.

start-of-authority (SOA) resource record A record that indicates the starting point or original point of authority for information stored in a zone. The SOA resource record is the first resource record created when adding a new zone. It also contains several parameters used by other computers that use Domain Name System (DNS) to determine how long they will use information for the zone and how often updates are required.

structured query language (SQL) A database sublanguage used to query, update, and manage relational databases. Although not a programming language in the same sense as C or Pascal, SQL can be used either in formulating interactive queries or embedded in an application as instructions for handling data. The SQL standard also contains components for defining, altering, controlling, and securing data.

subdomain A Domain Name System (DNS) domain located directly beneath another domain name (the parent domain) in the namespace tree. For example, example.microsoft.com would be a subdomain of the microsoft.com domain. A subdomain is also called a child domain.

subnet A portion of a network, which may be a physically independent network segment, that shares a classful network address with other portions of the network and is distinguished by a subnet number.

subnet mask A 32-bit value that allows the recipient of Internet Protocol (IP) packets to distinguish the network ID portion of the IP address from the host ID.

SVC *See* switched virtual circuit (SVC).

switched virtual circuit (SVC) A logical connection between end computers that uses a specific route across the network. Network resources are dedicated to the circuit, and the route is maintained until the connection is terminated. These are also known as point-to-multipoint connections.

synchronous A form of communication that relies on a timing scheme coordinated between two devices to separate groups of bits and transmit them in blocks called frames. Special characters are used to begin the synchronization and check its accuracy periodically. Because the bits are sent and received in a timed, controlled (synchronized) fashion, start and stop bits are not required. Transmission stops at the end of one transmission and starts again with a new one. It is a start/stop approach, and more efficient than asynchronous transmission. If an error occurs, the synchronous error detection and correction scheme implements a retransmission. However, because more sophisticated technology and equipment are required to transmit synchronously, it is more expensive than asynchronous transmission.

Synchronous Data Link Control (SDLC) The data link (data transmission) protocol most widely used in networks conforming to IBM's SNA. SDLC is a communications guideline that defines the format in which information is transmitted. As its name implies, SDLC applies to synchronous transmissions. SDLC is also a bit-oriented protocol and organizes information in structured units called frames.

Synchronous Optical Network (SONET) A fiber-optic technology that can transmit data at more than 1 gigabit per second. Networks based on this technology are capable of delivering voice, data, and video. SONET is a standard for optical transport formulated by the Exchange Carriers Standards Association (ECSA) for the ANSI.

System Monitor A tool that allows you to collect and view extensive data about the usage of hardware resources and the activity of system services on computers you administer.

Systems Network Architecture (SNA) A widely used communication framework developed by IBM to define network functions and establish standards for enabling its different models of computers to exchange and process data. SNA is a design philosophy that separates network communication into five layers. Each layer, like those in the similar ISO/OSI model, represents a graduated level of function moving upward from physical connections to applications software.

SYSVOL A shared directory that stores the server copy of the domain's public files, which are replicated among all domain controllers in the domain.

T

TCO *See* total cost of ownership (TCO).

TCP *See* Transmission Control Protocol (TCP).

TCP/IP *See* Transmission Control Protocol/Internet Protocol (TCP/IP).

TDI *See* transport driver interface (TDI).

Technet *See* Microsoft Technical Information Network (TechNet).

Telnet The command and program used to log on from one Internet site to another. The Telnet command and program bring the user to the logon prompt of another host.

Terminal Services Software services that allow client applications to be run on a server so that client computers can function as terminals rather than independent systems. The server provides a multisession environment and runs the Microsoft Windows-based programs being used on the clients.

throughput A measure of the data transfer rate through a component, connection, or system. In networking, throughput is a good indicator of the system's total performance because it defines how well the components work together to transfer data from one computer to another. In this case, the throughput would indicate how many bytes or packets the network could process per second.

Time to Live (TTL) A timer value included in packets sent over TCP/IP-based networks that tells routers when a packet has been forwarded too many times. For DNS, TTL values are used in resource records within a zone to determine how long requesting clients should cache, and use this information when it appears in a query response answered by a DNS server for the zone.

TokenTalk An expansion card that allows a Macintosh II to connect to an 802.5 Token Ring network.

total cost of ownership (TCO) The total amount of money and time associated with purchasing computer hardware and software and deploying, configuring, and maintaining the hardware and software. TCO includes hardware and software updates, training, maintenance, administration, and technical support.

tracert A trace route command-line utility that shows every router interface through which a TCP/IP packet passes on its way to a destination.

Transmission Control Protocol (TCP) The TCP/IP protocol for sequenced data. *See also* Transmission Control Protocol/Internet Protocol (TCP/IP).

Transmission Control Protocol/Internet Protocol (TCP/IP) An industry-standard suite of protocols providing communications in a heterogeneous environment. In addition, TCP/IP provides a routable, enterprise networking protocol and access to the Internet and its resources. It is a transport layer protocol that actually consists of several other protocols in a stack that operates at the session layer. Most networks support TCP/IP as a protocol.

transport driver interface (TDI) An interface that works between the file-system driver and the transport protocols, allowing any protocol written to TDI to communicate with the file-system drivers.

transport layer The fourth layer of the OSI reference model. It ensures that messages are delivered error-free, in sequence, and without losses or duplications. This layer repackages messages for efficient transmission over the network. At the receiving end, the transport layer unpacks the messages, reassembles the original messages, and sends an acknowledgment of receipt. *See also* Open Systems Interconnection (OSI) reference model.

transport protocols Protocols that provide for communication sessions between computers and ensure that data is able to move reliably between computers.

trunk A single cable, also called a backbone or segment.

trust relationship Trust relationships are links between domains that enable pass-through authentication, in which a user has only one user account in one domain, yet can access the entire network. User accounts and global groups defined in a trusted domain can be given rights and resource permissions in a trusting domain even though those accounts do not exist in the trusting domain's database. A trusting domain honors the logon authentication of a trusted domain.

TTL (Time to Live) *See* Time to Live (TTL).

U

UDP *See* User Datagram Protocol (UDP).

UNC (Universal Naming Convention) *See* Universal Naming Convention (UNC).

uninterruptible power supply (UPS) A device connected between a computer or another piece of electronic equipment and a power source, such as an electrical outlet. The UPS ensures that the electrical flow to the computer is not interrupted because of a blackout and, in most cases, protects the computer against potentially damaging events such as power surges and brownouts. Different UPS models offer different levels of protection. All UPS units are equipped with a battery and loss-of-power sensor. If the sensor detects a loss of power, it immediately switches over to the battery so that users have time to save their work and shut off the

computer. Most higher-end models have features such as power filtering, sophisticated surge protection, and a serial port so that an operating system capable of communicating with a UPS (such as Windows NT) can work with the UPS to facilitate automatic system shutdown.

Universal Naming Convention (UNC) The standard used for a full Windows 2000 name of a resource on a network. It conforms to the *server**share* syntax, where servername is the name of the server and sharename is the name of the shared resource. UNC names of directories or files can also include the directory path under the share name, with the following syntax: *server**share**directory**filename*.

UPS *See* uninterruptible power supply (UPS).

user account Consists of all of the information that defines a user on a network. This includes the user name and password required for the user to log on, the groups in which the user account has membership, and the rights and permissions the user has for using the system and accessing its resources.

User Datagram Protocol (UDP) A connectionless protocol responsible for end-to-end data transmission.

user groups Groups of users who meet online or in person to discuss installation, administration, and other network challenges for the purpose of sharing and drawing on each other's expertise in developing ideas and solutions.

user name A unique name identifying a user account to Microsoft Windows 2000. An account's user name must be unique among the other group names and user names within its own domain or workgroup.

V

virtual private network (VPN) A set of computers on a public network such as the Internet that communicate among themselves using encryption technology. In this way, their messages are safe from being intercepted and understood by unauthorized users. VPNs operate as if the computers were connected by private lines.

W

WAN *See* wide area network (WAN).

Web server A computer that is maintained by a system administrator or Internet service provider (ISP) and responds to requests from a user's Web browser.

wide area network (WAN) A computer network that uses long-range telecommunication links to connect networked computers across long distances.

Windows 2000 Advanced Server A powerful departmental and application server that provides rich network operations system (NOS) and Internet services. Advanced Server supports large physical memories, clustering, and load balancing.

Windows 2000 Datacenter Server The most powerful and functional server operating system in the Microsoft Windows 2000 family. It is optimized for large data warehouses, econometric analysis, large-scale simulations in science and engineering, and server consolidation projects.

Windows 2000 Professional A high-performance, secure network client computer and corporate desktop operating system that includes the best features of Microsoft Windows 98, significantly extending the manageability, reliability, security, and performance of Windows NT Workstation 4.0. Windows 2000 Professional can be used as a desktop operating system, networked in a peer-to-peer workgroup environment, or used as a workstation in a Windows 2000 Server domain environment.

Windows 2000 Server A file, print, and applications server, as well as a Web server platform that contains all of the features of Microsoft Windows 2000 Professional plus many new server-specific functions. This product is ideal for small- to medium-sized enterprise application deployments, Web servers, workgroups, and branch offices.

Windows Internet Name Service (WINS) A software service that dynamically maps Internet Protocol (IP) addresses to computer names (NetBIOS names). This allows users to access resources by name instead of requiring them to use IP addresses that are difficult to recognize and remember. WINS servers support clients running Microsoft Windows NT 4.0 and earlier versions of Microsoft operating systems.

winipcfg A diagnostic command specific to Microsoft Windows 95 and 98. Although this graphical user interface (GUI) utility duplicates the functionality of ipconfig, its GUI makes it easier to use. *See also* ipconfig.

WINS *See* Windows Internet Name Service (WINS).

workgroup A collection of computers grouped for sharing resources such as data and peripherals over a LAN. Each workgroup is identified by a unique name.

workstation Any networked Macintosh or PC using server resources on the network.

World Wide Web (the Web, WWW) The Internet multimedia service that contains a vast storehouse of hypertext documents written in HTML. *See also* Hypertext Markup Language (HTML).

X

X.25 A recommendation published by the CCITT that defines the connection between a terminal and a packet-switching network. A packet-switching network routes packets whose contents and format are controlled standards such as those defined in the X.25 recommendation. X.25 incorporates three definitions: the electrical connection between the terminal and the network, the transmission or link-access protocol, and the implementation of virtual circuits between network users. Taken together, these definitions specify a synchronous, full-duplex, terminal-to-network connection. Packets transmitted in such a network can contain either data or control commands. Packet format, error control, and other features are equivalent to portions of the HDLC protocol defined by the ISO. X.25 standards are related to the lowest three levels of the OSI reference model.

X.400 A CCITT protocol for international e-mail transmissions.

X.500 A CCITT protocol for file and directory maintenance across several systems.

XNS (Xerox Network System) A protocol developed by Xerox for its Ethernet LANs.

Z

zone In a Domain Name System (DNS) data-base, a zone is a subtree of the DNS database that is administered as a single, separate entity. This administrative unit can consist of a single domain or a domain with subdomains. A DNS zone administrator sets up one or more name servers for the zone.

zone database file The file where name-to-IP-address mappings for a zone are stored.

zone transfer The process by which Domain Name System (DNS) servers interact to maintain and synchronize authoritative name data. When a DNS server is configured as a secondary master for a zone, it periodically queries another DNS server configured as its source for the zone. If the version of the zone kept by the source is different, the secondary master server will pull zone data from its source DNS server to synchronize zone data.

zones Logical groupings of users and resources in an AppleTalk network.

Index

Note to the reader Italics are used to indicate references to illustrations.

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z

Microsoft®

MCSE Training Kit

Microsoft® Windows® 2000

Network Infrastructure Administration

הכנה למבחן הסמכה

#70-216

קרא לגבי התקליטור בהקדמה
ובקובץ ONCD שבתקליטור

תרגום, עריכה וייעוץ מקצועי: **צור ריכטר-לוין** Microsoft Certified Professional

עורכים: **צור ריכטר-לוין** Microsoft Certified Professional, **זהר עמיהוד** Microsoft Certified Professional

ייעוץ מקצועי: **שלום נייחסי** Microsoft Certified Professional + Internet, Microsoft Certified Professional Systems Engineer

ראש תחום רשתות בחברת הדרכה

סייע בתרגום פרק 11: **חנוך חנה**

עריכה ועיצוב: **ענבל אילני, טליה טופז**

עיצוב עטיפה: **ישראל מצגר**

שמות מסחריים

שמות המוצרים והשירותים המוזכרים בספר הינם שמות מסחריים רשומים של החברות שלהם. הוצאת הוד-עמי ו-Microsoft Press עשו כמיטב יכולתם למסור מידע אודות השמות המסחריים המוזכרים בספר זה ולציין את שמות החברות, המוצרים והשירותים. שמות מסחריים רשומים (registered trademarks) המוזכרים בספר צוינו בהתאמה.

Windows הינו מוצר רשום של חברת Microsoft

הודעה

ספר זה מיועד לתת מידע אודות מוצרים שונים. נעשו מאמצים רבים לגרום לכך שהספר יהיה שלם ואמין ככל שניתן, אך אין משתמעת מכך כל אחריות שהיא.

המידע ניתן "כמות שהוא" ("as is"). הוצאת הוד-עמי ו-Microsoft Press אינן אחראיות כלפי יחיד או ארגון עבור כל אובדן או נזק אשר ייגרם, אם ייגרם, מהמידע שבספר זה, או מהתקליטור שמצורף לו.

לשם שטף הקריאה כתוב ספר זה בלשון זכר בלבד.
ספר זה מיועד לגברים ונשים כאחד
ואין בכוונתנו להפלות או לפגוע בציבור המשתמשים/ות.

- **טלפון: 09-9564716**
- **פקס: 09-9571582**
- **דואר אלקטרוני**: info@hod-ami.co.il
- **אתר באינטרנט**: www.hod-ami.co.il

Microsoft®

MCSE Training Kit

Microsoft® Windows® 2000

Network Infrastructure Administration

הכנה למבחן הסמכה

#70-216

Microsoft®



MCSE Training Kit
Microsoft Windows 2000
Network Infrastructure Administration
By Microsoft Corporation

Original English language edition Copyright © 2000 by Microsoft Corporation

All rights published by arrangement with the original publisher, Microsoft Press, a division of Microsoft Corporation, Redmond, Washington, U.S.A.

Hebrew language edition published by
Hod-Ami Ltd. Copyright © 2001

© כל הזכויות שמורות

הוצאת הוד-עמי לספרי מחשבים בע"מ
ת.ד. 6108 הרצליה 46160
טלפון: 09-9564716 פקס: 09-9571582
www.hod-ami.co.il
info@hod-ami.co.il

אין להעתיק או לשדר בכל אמצעי שהוא ספר זה או קטעים ממנו בשום צורה ובשום אמצעי אלקטרוני או מכני, לרבות צילום והקלטה, אמצעי אחסון והפצת מידע, ללא אישור בכתב מאת ההוצאה, אלא לשם ציטוט קטעים קצרים בציון שם המקור.

מהדורה ראשונה 2001

All Rights Reserved
HOD-AMI Ltd.
P.O.B. 6108, Herzliya
ISRAEL, 2001

ISBN 965-361-280-8 מסת"ב

תוכן עניינים מקוצר

נספחים

תוכן העניינים

פרק 7: יישום DNS ‏(Domain Name System) 151

נספחים

אודות ספר זה

ברוכים הבאים לערכת ההדרכה לבחינת הסמכה 70-216 מבית Microsoft Press.

MCSE Training Kit -
Microsoft Windows 2000 Network Infrastructure Administration

ערכת הדרכה זו תדריך אותך כיצד לתכנן את תשתית הרשת שלך סביב תכונות הנתמכות על ידי Windows 2000. בערכה זו מוצגים ומושווים נושאים כגון פרוטוקולי רשת ושירותים, בהתאם לדרישות הארגון שלך. הדבר כולל את השימוש בפרוטוקול תואם IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange) לשם שילוב הרשת עם Novell NetWare. ההתמקדות העיקרית בפרוטוקולי רשת בספר זה היא בפרוטוקול TCP/IP (Transmission Control Protocol/Internet Protocol), מפני שהוא הפרוטוקול התקני באינטרנט, וגם מהווה את הבחירה הטובה ביותר עבור רשתות הארגון שלך. תלמד כיצד לנצל, לנהל ולהגדיר את TCP/IP ולהשתמש בתכונות כגון NetBIOS, WINS, DHCP ו-DNS. בנוסף תלמד גם כיצד להגדיר, לנהל, לאתר ולטפל בתקלות ניתוב וגישה מרחוק, כולל הגדרת VPN (Virtual Private Network).

כל פרק בספר זה מחולק לשיעורים. רוב השיעורים כוללים תרגולים מעשיים המאפשרים לך לתרגל או להדגים תפיסה מסוימת או ידע. כל פרק מסתיים בסיכום קצר של כל השיעורים בפרק ומספר שאלות סיכום הבוחנות את הידע שצברת מהחומר הנלמד בפרק.

הסעיף **תרגול** בפרק זה מספק הוראות התקנה חשובות המתארות את דרישות החומרה והתוכנה, להשלמת הלימוד בערכת לימוד זו. הוא גם מספק מידע אודות תצורת הרישות הנדרשת להשלמת חלק מהתרגולים המעשיים. קרא חלק זה בעיון לפני שתתחיל בשיעורים.

למי מיועד הספר?

ספר זה פותח עבור אנשי מקצוע בתחום טכנולוגיית המידע **I**nformation **T**echnology (IT), הנדרשים לעצב, לתכנן, ליישם ולתמוך במערכת Windows 2000 Server ברשתות ארגוניות, או למתכוונים להיבחן בבחינה 70-216 של Microsoft.

למה ללמוד בעברית כשהבחינה באנגלית?

אכן, בחינות ההסמכה של Microsoft נערכות באנגלית. גם חומר הלימוד המחולק במרכזי ההדרכה המורשים של Microsoft הוא באנגלית, ובכל זאת יש מקום לספר לימוד בעברית. הכיצד?

- המונחים שבספר מופיעים באנגלית ולידם הסבר בעברית.
- השאלות בסוף כל פרק הן באנגלית וגם בעברית.
- מילון המונחים, Glossary, הוא באנגלית.
- האינדקס הענק, בעזרתו תוכל למצוא כל דבר, הוא באנגלית.

דרישות מקדימות

הדרישות המקדימות לקורס זה הן:

- ידע עדכני ביסודות טכנולוגיות רשת.
- מומלץ ידע וניסיון בניהול רשתות מבוססות Windows NT 4.0.
- מומלץ לסיים בהצלחה את הקורס Microsoft Windows 2000 Server (70-215).

חומר עיוני

חומר העיון הבא עשוי להיות שימושי:

- Microsoft Windows 2000 Server Resource Kit.
- מערכת העזרה (Help) של Windows 2000 Server.
- אוסף מאמרים ו- White Papers הזמינים בכתובת האינטרנט http://www.microsoft.com/windows2000/guide/server/overview/.

אודות התקליטור המצורף

בתקליטור המצורף נמצאות שתי תיקיות משנה. האחת בשם EBook בה נמצאת הגירסה האלקטרונית המלאה של הספר באנגלית. השנייה Media בה נמצאים קבצי וידאו המסייעים בהדגמת המידע הנלמד בנושאי הקורס. ראה את הסעיף **תרגול** בהמשך הפרק, וקרא את הקובץ README.TXT שבתיקיה הראשית בתקליטור.

מצגות המולטימדיה מציגות חלק מנושאי המפתח בהם דן הספר. רצוי לצפות במצגות אלו כאשר תתבקש לכך, בעודך עובר על החומר הנלמד. גירסה מקוונת מלאה של ספר זה זמינה גם היא, ובה מיגוון אפשרויות צפייה. למידע נוסף אודות גירסה זו קרא את הסעיף **התקנת הספר המקוון** שבהמשך.

לפרטים נוספים על תוכן התקליטור פנה לקובץ ONCD בתיקיה הראשית שבתקליטור.

מבנה הספר

כל פרק פותח בסעיף **לפני שתתחיל**, המכין אותך להמשך הפרק.

➢ הפרקים בנויים משיעורים. בכל מקום שהדבר אפשרי כוללים השיעורים תרגולים המאפשרים לך להשתמש בידע שצברת עד כה, או כדי לסקור את החלק הנדון ביישום המתואר. כל התרגולים כוללים הליכי צעד-אחר-צעד המזוהים על ידי התבליט המופיע מימין לפסקה זו.

הסעיף **שאלות סיכום** בסוף כל פרק מאפשר לך לבחון מה למדת בשיעורי הפרק.

נספח A מכיל את כל שאלות הפרק והתשובות המתאימות באנגלית.

הערות

מספר סוגי הערות מופיעים בשיעורים:

- **טיפ** - כולל הסברים לתוצאות אפשריות או שיטות חליפיות.
- **חשוב** - כולל מידע חיוני להשלמת המטלה.
- **הערה** - כולל מידע נוסף והפניות.
- **הערת המתרגם** - כולל מידע נוסף הקשור בהתאמה לישראל, אך לא בהכרח נדרש לצורך הבחינה.
- **אזהרה** - כולל אזהרות על אפשרות אובדן נתונים.
- **הבהרה** - כולל הבהרות אודות מונח כלשהו המוזכר.

מוסכמות

המוסכמות הבאות משמשות בספר כולו.

מוסכמות כתיבה

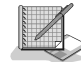
- תווים או פקודות להקלדה מופיעים באנגלית, בסדר הנדרש.
- שמות תיקיות וקבצים מופיעים בלועזית, כאשר האות הראשונה היא אות רישית (גדולה), פרט למקרים בהם אתה אמור להקליד אותם ישירות. אלא אם צוין אחרת, ניתן להשתמש באותיות קטנות להקלדת שם קובץ בתיבת דו-שיח או בשורת הפקודות.
- סיומות שמות קבצים מופיעות כולן באות קטנה.
- ראשי תיבות מופיעים באות גדולה.
- כיתוב באנגלית המוצמד לשמאל הוא דוגמת קוד, דוגמה של מה שמופיע במסך, או פקודות אותן עליך להקליד בשורת הפקודה או בקבצי האתחול.

❖ סוגריים מרובעים [ ] משמשים בפסוקי תחביר כדי לתחום פריט אופציונלי. לדוגמה, [filename] בתחביר פקודה מציין שניתן להקליד שם קובץ עם הפקודה. הקלד רק את הנתון שבתוך הסוגריים, לא את הסוגריים עצמם.

❖ סוגריים מסולסלים { } משמשים בפסוקי תחביר כדי לתחום פריט נדרש. הקלד רק את המידע בין הסוגריים, לא את הסוגריים עצמם.

❖ סמלים מייצגים חלקים מסוימים בספר:


מצגת מולטימדיה. תמצא את קובץ מצגת המולטימדיה האמור בתקליטור המצורף לספר זה.


תרגול. עליך לבצע את התרגול כדי לתת לעצמך אפשרות להשתמש בידע שצברת בשיעור זה.


שאלות סיכום. שאלות אלה מופיעות בסיומו של כל פרק ומאפשרות לך לבחון את שלמדת בשיעור זה. תמצא את התשובות לשאלות הסיכום ב**נספח A** שבסוף הספר.

מוסכמות מקלדת

❖ סימן חיבור (+) בין שני שמות מקשים, מורה שעליך ללחוץ על שניהם בו-זמנית. לדוגמה, "הקש Alt+Tab" משמעו שעליך ללחוץ על Alt ולהשאירו לחוץ בעודך מקיש על Tab.

❖ פסיק (,) בין שני שמות מקשים או יותר, משמעו שעליך להקיש על כל מקש ברצף, ולא יחדיו. לדוגמה "הקש Alt, F, X", משמעו שעליך להקיש ולשחרר כל מקש לפי תור. "הקש Alt+W, L", משמעו שעליך קודם להקיש על Alt ו-W ביחד, לשחררם ולהקיש על L.

❖ תוכל לבחור פקודות תפריט באמצעות המקלדת. הקש על מקש Alt להפעלת סרגל התפריטים, ואז בחר והקש לפי סדר את המקשים המתאימים לאות המוארת/מודגשת, או אות עם קו תחתי המציינים את שם התפריט ושם הפקודה. עבור כמה פקודות תוכל גם להקיש על שילוב מקשים המפורט בתפריט.

❖ ניתן לבחור או לבטל בחירה מתיבות סימון או לחצני אפשרויות בתיבות דו-שיח באמצעות המקלדת. הקש על מקש Alt, והקש על המקש המתאים לאות בעלת הקו התחתי בשם האפשרות. לחליפין, תוכל להקיש על Tab עד שהאפשרות תואר, ואז להקיש על מקש הרווח, כדי לבחור או לבטל בחירה מתיבת הסימון או מלחצן האפשרויות.

❖ ניתן לבטל את תצוגת תיבת הדו-שיח על ידי הקשה על מקש Esc.

סקירת פרקים ונספחים

קורס בקצב-אישי זה משלב טקסט תיאורי, הערות, הליכים מעשיים ושאלות סיכום, ללמדך להתקין ולהגדיר את Windows 2000 Server. הוא תוכנן לביצוע מההתחלה עד הסוף, אך תוכל לבחור מסלול לימוד אישי ולהשלים רק את החלקים המעניינים אותך (ראה בסעיף הבא, **מציאת נקודת ההתחלה הטובה ביותר עבורך**, מידע נוסף). אם תבחר את אפשרות מסלול הלימוד האישי, עיין בסעיף **לפני שתתחיל** בכל פרק. בכל תרגול מעשי הדורש פעולות מקדימות מפרקים קודמים, עיין בפרקים המתאימים.

הספר מחולק לפרקים הבאים:

- חלק **אודות ספר זה** מכיל סקירת הדרכה בקצב-אישי, ומציג את רכיבי ההדרכה. קרא חלק זה בעיון לקבלת ערך לימודי מירבי מהדרכה זו וכדי לתכנן איזה פרקים תלמד. חיוני להיצמד למידע ההתקנה המפורט ב**אודות ספר זה** להשלמה מוצלחת של התרגילים בערכת ההדרכה.
- פרק 1, **תכנון ועיצוב רשת Windows 2000**, מציג בפניך את פרוטוקולי הרשת והשירותים העיקריים לעיצוב תשתית רשת.
- פרק 2, **יישום TCP/IP**, מסביר כיצד להתקין ולהגדיר את פרוטוקול הרשת TCP/IP.
- פרק 3, **יישום NWLink**, מסביר כיצד להתקין ולהגדיר את פרוטוקול הרשת תואם-IPX/SPX, NWLink. בדרך כלל משמש פרוטוקול IPXSPX ברשתות LAN מבוססות שרתי Novell, ואילו NWLink מספק לך את הדרך לתקשר עם רשתות מסוג זה.
- פרק 4, **ניטור פעילות רשת**, מסביר כיצד להשתמש ביישום Network Monitor המגיע כחלק מ- Windows 2000.
- פרק 5, **יישום IPSec**, מסביר כיצד לאפשר, להגדיר ולנטר את IPSec, וכיצד להתאים באופן אישי את מדיניות וכללי IPSec.
- פרק 6, **הסדרת שמות מארחי רשת (Hosts)**, סוקר את השיטות השונות להסדרת שמות Hosts באמצעות TCP/IP.
- פרק 7, **יישום DNS**, מסביר כיצד משמש DNS להסדרת שמות ברשת שלך וברשת האינטרנט. Windows 2000 כוללת גירסה מורחבת של DNS.
- פרק 8, **שימוש ב-DNS בסביבת Windows 2000**, מסביר כיצד לעבוד עם אזורי DNS. זה כולל יישום אזור מואצל והגדרת אזורים לעדכונים דינמיים. תלמד גם כיצד להגדיר שרת DNS לעבודה כשרת מיטמון-בלבד, וכיצד לנטר ביצועי שרת.
- פרק 9, **יישום WINS**, מסביר כיצד משמש WINS להסדרת שמות NetBIOS ברשת שלך. תלמד גם כיצד לזהות את הרכיבים העיקריים של WINS, להתקין ולהגדיר WINS ולאתר ולטפל בתקלות בסביבת Windows 2000.
- פרק 10, **יישום DHCP**, מסביר כיצד משמש DHCP לניהול ולהגדרת מחשבי לקוח ברשת משרת Windows 2000 מרכזי אחד. תלמד כיצד לזהות את הרכיבים העיקריים של DHCP הן בלקוח והן בשרת, ולאתר ולטפל בתקלות DHCP.

- פרק 11, **מתן אפשרות גישה מרחוק ללקוחות**, מסביר כיצד ליישם את שירותי הגישה מרחוק, כדי לספק ללקוחותיך את האפשרות לגשת למשאבי רשת מביתם או ממיקום מרוחק אחר. תלמד כיצד ליישם חיבורים מאובטחים בטכניקות כגון VPN.
- פרק 12, **תמיכה ב-NAT**, מתאר את פרוטוקול תרגום כתובות הרשת NAT, אשר מאפשר לרשת עם כתובות פרטיות לגשת למידע באינטרנט באמצעות תהליך תרגום IP. תלמד כיצד להגדיר את הרשת הביתית/משרדית שלך לשתף חיבור יחיד לאינטרנט באמצעות NAT.
- פרק 13, **יישום שירותי אישורים**, מסביר את עקרונות האישורים, שהם המרכיבים היסודיים של תשתית המפתח הציבורי (Public Key Infrastructure) של Microsoft. תלמד כיצד להתקין ולהגדיר אישורים.
- פרק 14, **יישום אבטחת רשת ברמת הארגון**, מתאר את תכונות האבטחה של Windows 2000 וכיצד ליישם רשת מאובטחת עד כמה שניתן.
- נספח A, **Questions and Answers**, מהווה רשימה של כל השאלות בסעיפי **שאלות סיכום** בספר, עם התשובות.
- ה-**Glossary** כולל מונחים חשובים באנגלית ופירוט לגבי כל מונח.
- **אינדקס ענק**.

מצא את נקודת ההתחלה המתאימה ביותר עבורך

כיון שספר זה נועד להדרכה בקצב-אישי, תוכל לדלג על כמה שיעורים ולשוב אליהם מאוחר יותר. אולם, שים לב שבמקרים רבים, עליך להשלים תרגילים בכל פרק לפני השלמת תרגילים בפרקים מאוחרים יותר. השתמש בטבלה הבאה למציאת נקודת ההתחלה הטובה ביותר עבורך.

אם אתה	עקוב אחר מסלול הלימוד הזה
מתכוון לגשת למבחן ההסמכה Microsoft Certified Professional, שמספרו 70-216: יישום וניהול תשתיות רשת בסביבת Windows 2000.	קרא את סעיף **התחלת הקורס** ועקוב אחר **צעדי ההתקנה** שבסעיף **הוראות התקנה**. אחר כך, קרא פרקים 1 עד 14 לפי הסדר.
מעיין במידע על נושאים מסוימים מהבחינה.	השתמש בטבלאות שבהמשך.

Install, configure, and troubleshoot DNS

Skill Being Measured	Chapter	Lesson
Install the DNS Server service	7	4
Configure a root name server	7	2
Configure zones	8	1
Configure a caching-only server	8	2
Configure a DNS client	7	2
Configure zones for dynamic updates	8	1
Test the DNS Server Service	8	2
Implement a delegated zone for DNS	8	1
Manually create DNS resource records	7	5
Manage and monitor DNS	**8**	**2**

Installing, Configuring, Managing, Monitoring, and Troubleshooting DHCP in a Windows 2000 Network Infrastructure

Skill Being Measured	Chapter	Lesson
Install, configure, and troubleshoot DHCP		
Install the DHCP Server service	10	1
Create and manage DHCP scopes, superscopes, and multicast scopes	10	2
Configure DHCP for DNS integration	10	3
Authorize a DHCP server in Active Directory	10	4
Manage and monitor DHCP	**10**	**5**

Configuring, Managing, Monitoring, and Troubleshooting Remote Access in a Windows 2000 Network Infrastructure

Skill Being Measured	Chapter	Lesson
Configure and troubleshoot remote access		
Configure inbound connections	11	2
Create a remote access policy	11	2
Configure a remote access profile	11	2
Configure a VPN	11	4
Configure multilink connections	11	5
Configure Routing and Remote Access for DHCP integration	11	6
Manage and monitor remote access	**11** **14**	**7** **1**
Configure remote access security		
Configure authentication protocols	14	2
Configure encryption protocols	4 14	3 2
Create a remote access policy	11 14	2 2

Installing, Configuring, Managing, Monitoring, and Troubleshooting Network Protocols in a Windows 2000 Network Infrastructure

Skill Being Measured	Chapter	Lesson
Install, configure, and troubleshoot network protocols		
Install and configure TCP/IP	2	3
Install the NWLink protocol	3	4
Configure network bindings	3	4
Configure TCP/IP packet filters	**2**	**3**
Configure and troubleshoot network protocol security	**5** **14**	**2** **2**
Manage and monitor network traffic	**4** **14**	**2** **3**
Configure and troubleshoot IPSec		
Enable IPSec	5	1-2
Configure IPSec for transport mode	5	3
Configure IPSec for tunnel mode	5	3
Customize IPSec policies and rules	5	3
Manage and monitor IPSec	5	4

Installing, Configuring, Managing, Monitoring, and Troubleshooting WINS in a Windows 2000 Network Infrastructure

Skill Being Measured	Chapter	Lesson
Install, configure, and troubleshoot WINS	**9**	**1-4**
Configure WINS replication	**9**	**4**
Configure NetBIOS name resolution	**9** **9**	**1** **2**
Manage and monitor WINS	**9** **9**	**3** **4**

Installing, Configuring, Managing, Monitoring, and Troubleshooting IP Routing in a Windows 2000 Network Infrastructure

Skills Being Measured	Chapter	Lesson
Install, configure, and troubleshoot IP routing protocols		
Update a Windows 2000-based routing table by means of static routes	2 11	4 4
Implement demand-dial routing	11	2
Manage and monitor IP routing		
Manage and monitor border routing	2 11	4 1 and 7
Manage and monitor internal routing	2 11	4 6
Manage and monitor IP routing protocols	2 11 and 7	4 1 and 7

Installing, Configuring, and Troubleshooting NAT

Skills Being Measured	Chapter	Lesson
Install Internet Connection Sharing	**12**	**2**
Install NAT	**12**	**2 + 3**
Configure NAT properties	**12**	**3**
Configure NAT interfaces	**12**	**3**

Installing, Configuring, Managing, Monitoring, and Troubleshooting Certificate Services

Skills Being Measured	Chapter	Lesson
Install and configure Certificate Authority (CA)	**13**	**2**
Create certificates	**13**	**2**
Issue certificates	**13**	**2**
Revoke certificates	**13**	**3**
Remove the Encrypting File System (EFS) recovery keys	**13**	**3**

תרגול

קורס הדרכה זה כולל תרגולים מעשיים אשר יסייעו לך ללמוד אודות Windows 2000 Network Infrustructure Administration. כדי להשלים תרגולים אלה צריך שיהיה ברשותך מחשב בו מותקנת מערכת ההפעלה Windows 2000 Server.

קיימים מספר תרגולים בספר זה הדורשים שני מחשבים. השימוש במחשב השני נחוץ לשם השלמת מטרות השיעור. אם ברשותך מחשב אחד בלבד, קרא את הצעדים כולם כדי להכיר את הליכי התרגול טוב עד כמה שניתן.

מומלץ שתתקין את השרת כרשת נפרדת, כדי שלא תגרום לעומסים מיותרים על הרשת הפעילה, או שתשפיע על משתמשים ב-Domain הקיים. אבל, למרות זאת, ניתן להשתמש ברשת הקיימת עם השרת שלך.

אזהרה מספר תרגילים עשויים לדרוש ממך לבצע שינויים בשרתים. לכך עלולות להיות תוצאות בלתי רצויות אם אתה מחובר לרשת גדולה. בדוק ותאם עם מנהל הרשת, לפני ביצוע תרגילים אלה.

דרישות חומרה

על כל מחשב להיות בעל תצורת החומרה המינימלית הבאה. כל החומרה צריכה להופיע ברשימת החומרה התואמת (HCL, Hardware Compatibility List). הגירסה האחרונה והמעודכנת ביותר של HCL ניתנת להורדה מאתר HCL באינטרנט, בכתובת http://www.microsoft.com/hcl.

- Pentium 166Mhz
- 64MB זיכרון RAM לשם עבודה ברשת עם חמישה מחשבי לקוח; מומלץ על מינימום של 128MB זיכרון RAM עבור רוב סביבות הרישות.
- כונן דיסק קשיח בנפח 2GB.
- כונן תקליטורים במהירות 12x.
- מסך VGA המסוגל להפרדה של לפחות 800 x 600 (מומלצת הפרדה 1024x768).
- כונן דיסקטים "3.5, אלא אם חומרת המחשב תומכת באתחול מכונן התקליטורים.
- עכבר Microsoft או התקן הצבעה תואם.

דרישות תוכנה

תצטרך עותק של תקליטור ההתקנה של Windows 2000 Server.

הוראות התקנה

המידע הבא הוא רשימת תיוג (Check List) של משימות שעליך לבצע כדי להכין את המחשב שלך לשיעורים בספר זה. אם אין לך ניסיון בהתקנת Windows 2000 או מערכת הפעלה לרשת אחרת, ייתכן ותדרש לך עזרתו של מנהל מערכת מנוסה. לאחר שתשלים משימה, סמן את תיבת הסימון לידה. בהמשך מופיעים הסברים צעד-אחר-צעד לגבי כל משימה.

- ❏ צור תקליטוני (דיסקטים) התקנה של Windows 2000 Server.
- ❏ הפעל את שגרות הקדם-העתקה (Pre-Copy) ומצב טקסט בהתקנה (Text Mode Setup).
- ❏ הפעל את שלב ממשק המשתמש הגרפי ושלב איסוף הנתונים של התקנת Windows 2000 Server.
- ❏ השלם את שלב התקנת רכיבי הרישות של תוכנית ההתקנה של Windows 2000 Server.
- ❏ השלם את שלב התקנת החומרה של תוכנית ההתקנה של Windows 2000 Server.

הערה מידע ההתקנה המסופק להלן יסייע לך להכין מחשב לצורך לימוד נושאי ספר זה. חלק זה לא נועד ללמדך את אופן התקנת המוצר. למידע מפורט אודות התקנת Windows 2000 Server קרא את הספר **Windows 2000 Server הכנה לבחינת הסמכה 70-215**, גם הוא בהוצאת **הוד-עמי**.

התקנת Windows 2000 Server

כדי להשלים את התרגולים בספר זה, עליך להתקין את Windows 2000 Server במחשב בו לא קיימות מחיצות מפורמטות. בעת תהליך ההתקנה תוכל להיעזר בתוכנית ההתקנה של Windows 2000 Server כדי ליצור מחיצה בכונן הדיסק הקשיח שלך, בה תתקין את Windows 2000 Server כשרת עצמאי בקבוצת עבודה.

השלם את התהליכים הבאים במחשב בו פועלת גירסה של MS-DOS או גירסה כלשהי של Windows, אשר מאפשרת גישה לתיקיה Bootdisk שבתקליטור ההתקנה של Windows 2000 Server. אם חומרת המחשב שלך מאפשרת אתחול מתקליטור, תוכל לבצע את ההתקנה ללא תקליטוני ההתקנה. כדי להשלים תרגול זה כפי שהוא מתואר כאן, יש לבטל ב-BIOS המערכת את אפשרות האתחול מכונן התקליטורים.

חשוב תרגיל זה דורש ארבעה דיסקטים "3.5 מפורמטים, בנפח של 1.44MB כל אחד. אם תשתמש בדיסקטים המכילים נתונים, יימחקו נתונים אלה ללא כל אזהרה נוספת.

➢ כדי ליצור דיסקטים של התקנה עבור תוכנית ההתקנה של Windows 2000 Server

1. הדבק תוויות כדלקמן על ארבעה דיסקטים מפורמטים 1.44MB :

   דיסקט התקנה Windows 2000 Server מס' 1

   דיסקט התקנה Windows 2000 Server מס' 2

   דיסקט התקנה Windows 2000 Server מס' 3

   דיסקט התקנה Windows 2000 Server מס' 4
2. הכנס את תקליטור Windows 2000 Server לכונן התקליטורים.
3. אם מופיעה תיבת הדו-שיח של תקליטור Windows 2000 המנחה אותך להתקין או לשדרג ל-Windows 2000, לחץ No.
4. פתח חלון שורת פקודה (Command Prompt).
5. בשורת הפקודה, עבור לכונן התקליטורים שלך. לדוגמה, אם האות המייצגת את כונן התקליטורים שלך היא E, הקלד **e:** והקש Enter.
6. במנחה הפקודה, עבור לתיקיה Bootdisk, על ידי הקלדת הפקודה cd bootdisk והקשה על Enter.
7. אם אתה מכין את דיסקטים אתחול ההתקנה במחשב המפעיל MS-DOS, מערכת הפעלה 16 סיביות של Windows או מערכת הפעלה Windows 9x, הקלד makeboot a: (כאשר :A הוא שם כונן הדיסקטים) והקש Enter. אם אתה יוצר את דיסקטים אתחול ההתקנה במחשב Windows NT או Windows 2000, הקלד את הפקודה makebt32 a: (כאשר :A הוא שם כונן הדיסקטים) והקש Enter. Windows 2000 תציג הודעה המציינת שתוכנית זו יוצרת ארבעה דיסקטים להתקנת Windows 2000. כמו כן תופיע הודעה שנדרשים ארבעה דיסקטים High Density (מפורמטים בצפיפות גבוהה).
8. הקש על מקש כלשהו להמשך. Windows 2000 תציג הודעה המנחה אותך להכניס את הדיסקט שיהיה Windows 2000 Setup Boot Disk (דיסקט אתחול ההתקנה של Windows 2000).
9. הכנס את הדיסקט עם התווית **דיסקט התקנה Windows 2000 Server מס' 1** (מפורמט וריק) לכונן הדיסקטים, והקש על מקש כלשהו להמשך. לאחר ש-Windows 2000 תיצור את הדיסקט, היא תציג הודעה המנחה אותך להכניס את הדיסקט עם תווית **דיסקט התקנה Windows 2000 Server מס' 2**.
10. הוצא את דיסקט מספר 1, הכנס את הדיסקט המפורמט הריק עם התווית **דיסקט התקנה Windows 2000 Server מס' 2** לכונן הדיסקטים, והקש מקש כלשהו להמשך. לאחר ש-Windows 2000 תיצור את הדיסקט, היא תציג הודעה המנחה אותך להכניס את הדיסקט עם התווית **דיסקט התקנה Windows 2000 Server מס' 3**.

11. הוצא את דיסקט מספר 2, הכנס את הדיסקט עם התווית **דיסקט התקנה Windows 2000 Server מס' 3** לכונן הדיסקטים, והקש מקש כלשהו להמשך. לאחר ש-Windows 2000 תיצור את הדיסקט, היא תציג הודעה המנחה אותך להכניס את הדיסקט עם תווית **דיסקט התקנה Windows 2000 Server מס' 4**.

12. הוצא את דיסקט מספר 3, הכנס את הדיסקט עם התווית **דיסקט התקנה Windows 2000 Server מס' 4** לכונן הדיסקטים, והקש מקש כלשהו להמשך.

    לאחר ש-Windows 2000 תיצור את הדיסקט, היא תציג הודעה שהליך יצירת הדיסקטים הסתיים.

13. בשורת הפקודה, הקלד Exit והקש Enter.

    הוצא את הדיסקט מכונן הדיסקטים ואת התקליטור מכונן התקליטורים.

➢ כדי להפעיל נוהל קדם-העתקה והגדרת מצב טקסט בתוכנית ההתקנה של Windows 2000 Server

---

הערה תרגיל זה יוצא מנקודת הנחה שבמחשב שלך לא מותקנת מערכת הפעלה כלשהי, כונן הדיסק הקשיח אינו מחולק למחיצות ושאפשרות האתחול מכונן התקליטורים, במידה ונתמכת על ידי חומרת המחשב, מבוטלת.

---

1. הכנס את הדיסקט המסומן "דיסקט התקנה Windows 2000 Server מס' 1" לכונן הדיסקטים, הכנס את תקליטור Windows 2000 Server לכונן התקליטורים, ואתחל את Server01.

   לאחר שהמחשב מתחיל, תוכנית ההתקנה של Windows 2000 תציג הודעה קצרה המציינת שתצורת המערכת בבדיקה, ואז יופיע מסך ההתקנה של Windows 2000.

   שים לב שהסרגל האפור בתחתית המסך מעיד שהמחשב בבדיקה ושמערכת Windows 2000 Executive נטענת. זו הגירסה המינימלית של Kernel (ליבת) Windows 2000.

2. כאשר תתבקש על ידי המערכת, הכנס את דיסקט התקנה מס' 2 לכונן הדיסקטים והקש Enter. תוכנית ההתקנה מציינת שהיא טוענת את HAL, גופנים, נתונים ייחודים לאזור, מנהלי התקן אפיק (bus drivers) ורכיבי תוכנה נוספים לתמיכה בלוח האם, אפיק וחומרה נוספת במחשב שלך. תוכנית ההתקנה טוענת גם את קבצי התוכנה של Windows 2000 Setup.

3. כאשר תתבקש על ידי המערכת, הכנס את דיסקט התקנה מס' 3 לכונן הדיסקטים והקש Enter. תוכנית ההתקנה מציינת שהיא טוענת את בקרי המנהלים של התקני הכוננים (disk drive controller drivers). לאחר טעינת ה-drive controllers, תוכנית ההתקנה מאתחלת את מנהלי ההתקנים (drivers) המתאימים לתמיכה בגישה לכוננים. תוכנית ההתקנה עלולה להשתהות מספר פעמים במהלך פעולה זו.

4. כאשר תתבקש על ידי המערכת, הכנס את דיסקט התקנה מס׳ 4 לכונן הדיסקטים והקש Enter.

תוכנית ההתקנה טוענת את מנהלי ההתקנים (drivers) של הציוד ההיקפי, כגון מנהל ההתקן (driver) של כונן הדיסקטים ומערכת הקבצים, ואז היא מאתחלת את Windows 2000 Executive וטוענת את שאר תוכנית ההתקנה של Windows 2000.

אם אתה מתקין גרסת הדגמה (Evaluation Version) של Windows 2000, יופיע מסך הודעות ובו הודעה שאתה עומד להתקין גרסת הדגמה של Windows 2000.

5. קרא את הודעת ההתקנה, והקש Enter להמשך. תוכנית ההתקנה תציג את מסך Welcome To Setup (ברוך הבא להתקנה).

שים לב, שבנוסף להתקנת Windows 2000, תוכל להשתמש בתוכנית ההתקנה של Windows 2000 לתיקון התקנה פגומה של Windows 2000.

6. קרא את הודעת Welcome To Setup והקש Enter להתחלת שלב ההתקנה של Windows 2000 Setup. תוכנית ההתקנה תציג את הסכם הרשיון.

7. קרא את הסכם הרשיון, תוך הקשה על Page Down, כדי לגלול לתחתית המסך.

8. בחר I Accept The Agreement (אני מקבל את ההסכם) באמצעות F8.

תוכנית ההתקנה תציג את מסך ההתקנה של Windows 2000 Server, ותנחה אותך לבחור אזור פנוי בדיסק או מחיצה קיימת, בה תתקין את Windows 2000. שלב זה בתוכנית ההתקנה הוא אמצעי ליצירה ומחיקת מחיצות בדיסק הקשיח.

אם במחשב אין מחיצות (כנדרש עבור תרגיל זה), תראה שהדיסק המופיע על המסך כולל מחיצה לא מפורמטת.

9. ודא שהמחיצה הלא מחולקת מוארת, והקש C.

תוכנית ההתקנה תציג את מסך ההתקנה של Windows 2000, תאשר שבחרת ליצור מחיצה חדשה באזור שאינו מחולק למחיצות, ותיידע אותך מה הגודל המזערי והמירבי של המחיצה שתוכל ליצור.

10. הגדר את גודל המחיצה שברצונך ליצור (2GB לפחות), והקש Enter להמשך.

תוכנית ההתקנה תציג את מסך ההתקנה של Windows 2000, ובו תוצג המחיצה החדשה כ: C:\New (Unformatted).

הערה אף שתוכל ליצור מחיצות נוספות מהשטח הלא מחולק שנותר בעת ההתקנה, מומלץ שתבצע פעולות חלוקה נוספות לאחר התקנת Windows 2000. לחלוקת דיסקים קשיחים למחיצות לאחר ההתקנה השתמש ב- Snap-In (תוסף התוכנה) Disk Management.

---

11. ודא שהמחיצה החדשה מוארת, והקש Enter.

כעת תתבקש לבחור מערכת קבצים עבור המחיצה.

12. השתמש במקשי החיצים לבחירת Format The Partition Using The NTFS File System, והקש Enter.

תוכנית ההתקנה מפרמטת את המחיצה החדשה במערכת הקבצים NTFS. לאחר פרמוט המחיצה, תוכנית ההתקנה סורקת את הדיסק לאיתור פגמים פיסיים העלולים לגרום לתוכנית ההתקנה להיכשל, ואז מעתיקה קבצים לדיסק הקשיח. הליך זה יארך מספר דקות.

בסופו של דבר, תוכנית ההתקנה תציג את מסך ההתקנה של Windows 2000 Server. מד התקדמות אדום מבצע ספירה לאחור במשך 15 שניות לפני שתוכנית ההתקנה מאתחלת את המחשב.

13. הוצא את דיסקט ההתקנה מהכונן.

חשוב אם המחשב שלך תומך באתחול מכונן התקליטורים ותכונה זו לא בוטלה (Disabled) ב- BIOS, המחשב יאתחל מתקליטור ההתקנה של Windows 2000 Server לאחר שתוכנית ההתקנה של Windows 2000 תתחיל מחדש. כתוצאה מכך תוכנית ההתקנה תתחיל שוב מההתחלה. אם דבר זה קורה, הוצא את התקליטור מהכונן, ואתחל את המחשב פעם נוספת.

---

14. תוכנית ההתקנה מעתיקה קבצים נוספים, מאתחלת את המחשב שנית וטוענת את אשף Windows 2000 Setup.

➢ כדי להפעיל את מצב GUI ואיסוף נתונים בתוכנית ההתקנה של Windows 2000 Server

---

הערה הליך זה מתחיל את החלק הגרפי של תוכנית ההתקנה במחשב שלך .

---

1. לחץ Next במסך אשף ההתקנה Welcome to The Windows 2000 Setup Wizard, להתחלת איסוף נתונים אודות המחשב שלך.

תוכנית ההתקנה מגדירה תיקיית NTFS והרשאות עבור קבצי מערכת ההפעלה, מאתרת את התקני החומרה במחשב, ואז מתקינה ומגדירה מנהלי התקנים לתמיכה בחומרה שאותרה. הליך זה אורך מספר דקות.

2. בחלון Regional Settings, ודא שהגדרות המערכת, הגדרות המשתמש והמקלדת נכונות עבור השפה והאזור שלך, ולחץ Next.

הערה תוכל לשנות את ההגדרות האזוריות לאחר התקנת Windows 2000, באמצעות היישומון Regional Options בלוח הבקרה.

תוכנית ההתקנה תציג חלון Personalize Your Software, ותתבקש להקליד את שמך ואת שם הארגון שלך. תוכנית ההתקנה משתמשת בשם הארגון שלך ליצירת שם ברירת מחדל עבור המחשב. יישומים רבים שתתקין בעתיד ישתמשו בנתון זה לרישום מוצריהם וזיהוי מסמכים.

3. בשדה Name הקלד את שמך; בשדה Organization, הקלד את שם הארגון; לחץ Next.

הערה **אם מופיע מסך** Your Product Key, **הקלד את קוד המוצר** (Product Key) **המסופק על אריזת תקליטור ההתקנה של** Windows 2000 Server, **ולחץ** Next.

תוכנית ההתקנה מציגה את מסך Licensing Mode, ומנחה אותך לבחור סוג רשיון. ברירת המחדל הוא רשיון Per Server (לפי שרת). תוכנית ההתקנה מנחה אותך להקליד את מספר הרשאות המשתמשים שרכשת עבור שרת זה.

4. לחץ על לחצן האפשרויות Per Server Number of Concurrent Connections (מספר חיבורים בו-זמניים לשרת זה) והקלד **5** עבור מספר החיבורים הנוכחיים. לחץ Next.

חשוב **האפשרויות** Per Server **והערך 5** **עבור מספר הלקוחות האפשריים בו-זמנית, הם ערכים מומלצים המשמשים בתרגיל זה. עליך להשתמש במספר חוקי של חיבורים בו-זמניים, בהתאם לרשיונות שרכשת. תוכל גם לבחור בהגדרה** Per-Seat **(לפי מושב) במקום** Per Server **(לפי שרת).**

תוכנית ההתקנה תציג את מסך Computer Name And Administrator Password (שם מחשב וסיסמת מנהל (administrator)).

שים לב שתוכנית ההתקנה משתמשת בשם הארגון שלך ליצירת שם מוצע עבור המחשב.

5. בשדה Computer Name הקלד **SERVER1**.

Windows 2000 תציג את שם המחשב באותיות גדולות (רישיות) בלי קשר לאופן ההקלדה.

אזהרה במידה ומחשב זה מחובר לרשת, היוועץ במנהל הרשת שלך קודם להקצאת שם למחשב זה.

בהמשך ספר זה, ההתייחסות תהיה למחשב שרת Server1. אם לא קראת למחשב שלך Server1, בכל מקום שיש התייחסות לשרת Server1, תיאלץ להחליפו בשם השרת שנתת.

6. בשדה Administrator Password ובשדה Confirm Password, הקלד password (באותיות קטנות) ולחץ Next. בניגוד לשמות משתמש שאינם תלויי-רישיות (Case Insensitive), סיסמאות הן תלויות-רישיות (Case Sensitive).

במהלך ערכת לימוד עצמית זו, סיסמת חשבון מנהל המערכת (Administrator) תהיה password. בסביבת עבודה אמיתית, יש להשתמש בסיסמה מורכבת עבור חשבון מנהל הרשת (כזו שתהיה קשה לניחוש). Microsoft ממליצה שילוב אותיות גדולות וקטנות, ספרות ותווים מיוחדים (לדוגמה, Lp6*g9).

תוכנית ההתקנה תציג את מסך Windows 2000 Components, ותציין איזה רכיבי מערכת Windows 2000 היא תתקין.

תוכל להתקין רכיבים נוספים לאחר התקנת Windows 2000, באמצעות יישומון Add/Remove Programs בלוח הבקרה. ודא שמותקנים רק רכיבים שנבחרו על ידי ברירת המחדל בעת ההתקנה. בהמשך הלימוד, תתקין רכיבים נוספים.

7. במסך Windows 2000 Components לחץ Next.

8. אם תוכנית ההתקנה איתרה מודם בעת ההתקנה, היא תציג את מסך הגדרות החיוג של המודם.

9. אם מופיע מסך Modem Dialing Information (מסך נתוני החיוג של המודם), הכנס את קוד אזור החיוג, ולחץ Next. יופיע מסך Date and Time Settings (הגדרת תאריך ושעה).

חשוב **שירותי** Windows 2000 **מבצעים מטלות רבות שהצלחתן מותנית בהגדרת התאריך והשעה של המחשב. ודא בחירה נכונה של אזור הזמן שלך, למניעת תקלות עתידיות.**

---

10. הכנס את ערכי התאריך, הזמן והגדרת אזור הזמן ולחץ Next. יופיע מסך Network Settings ותוכנית ההתקנה תתקין את רכיבי הרשת.

➢ השלמת שלב התקנת רכיבי הרשת בתוכנית ההתקנה של Windows 2000 Server

רשת היא חלק אינטגרלי ב- Windows 2000 Server וניתן לבחור ולהגדיר תצורות רבות עבורה. בחלק זה, מוגדרת תצורת רשת בסיסית. בתרגילים בהמשך, תתקין רכיבי רשת נוספים.

1. במסך Networking System, ודא בחירת Typical Settings, ולחץ Next להתחלת ההתקנה של רכיבי הרשת של Windows.

   הגדרות אלו יתקינו רכיבי רשת המשמשים לגישה ושיתוף במשאבי הרשת והן מגדירות את פרוטוקול TCP/IP לקבלת כתובת IP אוטומטית משרת DHCP ברשת.

   תוכנית ההתקנה תציג מסך בו תוכל לבחור אם לצרף את המחשב ל-Workgroup או ל-Domain, ותנחה אותך להצטרף לאחד משניהם.

2. במסך Workgroup או Domain, ודא שנבחר לחצן אפשרויות No, This Computer Is Not On A Network Or Is On A Network Without A Domain (לא, מחשב זה אינו ברשת או שהוא ברשת ללא Domain), ושם קבוצת העבודה הוא WORKGROUP, ולחץ Next. תוכנית ההתקנה תציג את מסך Installing Components (התקנת רכיבים), תוך שהיא מציגה את המצב בעת ההתקנה והגדרת שאר רכיבי מערכת ההפעלה בהתאם לברירות שהגדרת. פעולה זו אורכת מספר דקות.

   תוכנית ההתקנה תציג כעת את מסך Performing Final Tasks (מבצעת מטלות אחרונות), המראה את המצב בעת סיום העתקת קבצים, יצירת שינויי תצורה ושמירתם ומחיקת קבצים זמניים. מחשבים בעלי תצורה שאינה מעבר לדרישות הסף של החומרה, עלולים לדרוש 30 דקות או יותר להשלמת שלב זה של ההתקנה.

   עתה תציג תוכנית ההתקנה את מסך אשף Completing The Windows Setup.

3. הוצא את תקליטור Windows 2000 Server מכונן התקליטורים, ולחץ Finish.

חשוב אם המחשב שלך תומך באתחול מכונן התקליטורים ותכונה זו לא בוטלה (Disabled) ב- BIOS, המחשב יאתחל מתקליטור ההתקנה של Windows 2000 Server לאחר שתוכנית ההתקנה של Windows 2000 תתחיל מחדש. כתוצאה מכך, תוכנית ההתקנה תתחיל שוב מההתחלה. אם דבר זה קורה, הוצא את התקליטור מהכונן, ואתחל את המחשב שנית.

Windows 2000 מתחילה שנית ומפעילה את גרסת Windows 2000 Server החדשה שהותקנה.

➢ כדי להשלים את שלב התקנת החומרה בתוכנית ההתקנה של Windows 2000 Server

במהלך שלב אחרון זה של ההתקנה, תאותר כל חומרת Plug and Play (הכנס-הפעל) שלא אותרה בשלבים הקודמים של ההתקנה.

1. עם סיום שלב האתחול, הכנס למחשב על ידי הקשה על שילוב המקשים Ctrl+Alt+Delete.
2. בתיבת דו-שיח Enter Password, בשדה User Name הקלד **Administrator**, ובשדה Password הקלד **password**.
3. לחץ OK.
4. אם Windows 2000 מאתרת חומרה שלא אותרה בעת ההתקנה, יופיע מסך אשף Found New Hardware (נמצאה חומרה חדשה), המעיד כי Windows 2000 מתקינה את מנהלי ההתקן (drivers) המתאימים.

   אם מופיע מסך אשף Found New Hardware, ודא שתיבת סימון Restart The Computer When I Finish (אתחל את המחשב כשאסיים) אינה מסומנת, ולחץ Finish לסיום פעולת האשף Found New Hardware.

   Windows 2000 תציג את תיבת דו-שיח Microsoft Windows 2000 Configure Your Server. מתיבת סימון זו תוכל להגדיר מיגוון אפשרויות מתקדמות ושירותים.
5. לחץ על לחצן האפשרויות I Will Configure This Server Later (אגדיר שרת זה מאוחר יותר), ולחץ Next.
6. במסך הבא שמופיע, בטל את הסימון מתיבת הסימון Show This Screen At Startup (הצג מסך זה בעת האתחול).
7. סגור את מסך Configure Your Server.

   השלמת את התקנת Windows 2000 Server והינך עובד בו כמנהל המערכת.

אזהרה אם המחשבים שלך מהווים חלק מרשת גדולה, עליך לוודא עם מנהל הרשת שלך ששמות המחשבים, שמות ה-Domains ומידע אחר בו נעשה שימוש בעת התקנת והגדרת המערכת בפרק זה אינם מפריעים לפעולה התקינה של הרשת. אם אכן נוצרת הפרעה (כגון התנגשויות למיניהן), בקש ממנהל הרשת ערכים חליפיים והשתמש בערכים אלה לכל אורך התרגולים בספר.

הפעלת מצגות מולטימדיה

התקליטור המצורף לספר זה מכיל מספר מצגות מולטימדיה, בהן תוכל לצפות על ידי הפעלת קבצים מהתקליטור. במקומות המיועדים בספר תמצא הנחייה לקובץ אותו יש להפעיל.

➢ **כדי לצפות במצגת**

1. הכנס את התקליטור המצורף לספר לכונן התקליטורים במחשב.
2. לחץ Start, בחר Run, ובתיבת הטקסט Open הקלד את הפקודה E:\Media\demo_filename (כאשר :E היא האות המייצגת את כונן התקליטורים שלך ואילו demo_filename הוא שם הקובץ המצוין בספר).

התקנת הספר המקוון

בתקליטור המצורף לספר זה תמצא גם גירסה מקוונת של ספר זה, בה ניתן לצפות באמצעות Internet Explorer 5.x (מצורפת בתקליטור).

➢ **כדי להשתמש בגירסה המקוונת של הספר**

1. הכנס את התקליטור המצורף לספר לכונן התקליטורים במחשב.
2. לחץ Start, בחר Run, ובתיבת הטקסט Open הקלד את הפקודה E:\EBook\setup.exe (כאשר :E היא האות המייצגת את כונן התקליטורים שלך).

   פעולה זו תתקין בתפריט Start שלך קיצור דרך לספר המקוון.
3. לחץ OK כדי לצאת מאשף ההתקנה.

הערה כדי לצפות בספר המקוון, התקליטור צריך להיות בכונן התקליטורים.

הדרכה טכנית לאנשי מחשבים

הדרכה טכנית זמינה במיגוון דרכים, באמצעות כיתות הדרכה, הדרכה מקוונת, או לימוד בקצב-אישי באלפי אתרים ברחבי העולם.

לימוד בקצב-אישי

עבור לומדים בעלי מוטיבציה המוכנים להתמודד עם האתגר, לימוד בקצב-אישי היא השיטה הגמישה והחסכונית ביותר להגדלת הידע והכישורים. ספר זה, שהינו ספר לימוד בקצב-אישי, יכול גם לשמש כחומר עזר נלווה לקורס הנערך במרכז הדרכה.

הדרכה מקוונת

לחלופה גמישה יותר מכיתות לימוד, פנה להדרכה מקוונת. זה קרוב כמו האינטרנט ומוכן מתי שאתה מוכן. למד בקצב שלך ולפי לוח הזמנים שלך בכיתה וירטואלית, לעיתים קרובות עם גישה קלה למורה מקוון. תוכל לרכוש את המיומנות הנדרשת ללא עזיבת שולחן העבודה. הדרכה מקוונת מכסה מיגוון מוצרי Microsoft וטכנולוגיות. היא כוללת אפשרויות הנעות מ-Microsoft Official Curriculum (תוכנית הלימוד הרשמית של Microsoft) לאפשרויות שאינן זמינות בשום מקום אחר. זוהי הדרכה לפי דרישה, עם גישה למשאבי לימוד 24 שעות ביום. הדרכה מקוונת זמינה באמצעות מרכזי הדרכה מוסמכים של חברת Microsoft.

הערות, שאלות, רעיונות

לא נחסך כל מאמץ להבטחת הדיוק של ספר זה והתקליטור המצורף אליו. אם יש לך הערות, שאלות או רעיונות הנוגעים לספר זה או לתקליטור המצורף, אנא שלח אותם ל**הוצאת הוד-עמי** באחת השיטות הבאות:

דואר אלקטרוני:

support@hod-ami.co.il

ובשורת הנושא (Subject) הקלד את הנושא **59311**.

דואר רגיל:

הוצאת הוד-עמי לספרי מחשבים בע"מ
ת.ד. 6108
הרצליה 46160

אנא שים לב שהכתובות הבאות אינן מספקות תמיכה. למידע נוסף על תמיכה בתוכנות Microsoft, בקר באתר http://www.microsoft.com/israel/support.